AVG AntiVirus

Manuale per l'utente

Revisione documento AVG.01 (9/16/2015)

Sommario

1. Introduzione

Questa guida per l'utente fornisce la documentazione completa relativa a **AVG AntiVirus**.

Grazie ai diversi livelli di protezione per tutte le attività svolte in linea offerti da

AVG AntiVirus offre la protezione in tempo reale dalle minacce odierne più sofisticate. È possibile chattare, scaricare e scambiare i file in tutta tranquillità, nonché giocare e guardare video senza preoccupazioni né interruzioni, scaricare, condividere file e inviare messaggi in modo sicuro, utilizzare i social network o esplorare ed eseguire ricerche con una protezione in tempo reale.

Sono inoltre disponibili altre fonti di informazioni:

- ***File della Guida***: una sezione *Risoluzione dei problemi* è disponibile direttamente nel file della Guida incluso in **AVG AntiVirus** *(per aprire il file della Guida, premere il tasto F1 in qualsiasi finestra di dialogo nell'applicazione)*. Questa sezione fornisce un elenco delle situazioni che con maggiore frequenza spingono un utente a ricercare assistenza professionale per un problema tecnico. Selezionare la situazione che descrive meglio il problema corrente e fare clic sul collegamento per aprire le istruzioni dettagliate per la risoluzione del problema.

- ***Centro di assistenza del sito Web di AVG***: in alternativa, è possibile ricercare la soluzione al problema nel sito Web di AVG (*http://www.avg.com/*). Nella sezione ***Assistenza*** sono contenuti una panoramica di gruppi tematici che trattano problemi commerciali e tecnici, una sezione strutturata di domande frequenti e tutti i contatti disponibili.

- ***AVG ThreatLabs***: un sito Web specifico correlato ad AVG (*http://www.avg.com/about-viruses*) dedicato ai virus, che fornisce una panoramica strutturata delle informazioni relative alle minacce online. Sono inoltre disponibili istruzioni sulla rimozione di virus e spyware e consigli relativi alla protezione.

- ***Forum di discussione***: è inoltre possibile utilizzare il forum di discussione degli utenti AVG disponibile all'indirizzo http://community.avg.com/.

2. Requisiti per l'installazione di AVG

2.1. Sistemi operativi supportati

AVG AntiVirus consente di proteggere le workstation che eseguono i seguenti sistemi operativi:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (tutte le edizioni)
- Windows 7 (tutte le edizioni)
- Windows 8 (tutte le edizioni)
- Windows 10 (tutte le edizioni)

(ed eventuali Service Pack successivi per sistemi operativi specifici)

***Nota**: il componente Identità non è supportato in Windows XP x64. Su questo sistema operativo è possibile installare AVG AntiVirus, ma solo senza il componente IDP.*

2.2. Requisiti hardware minimi e consigliati

Requisiti hardware minimi per **AVG AntiVirus**:

- CPU Intel Pentium da 1,5 GHz o superiore
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) di memoria RAM
- 1,3 GB di spazio libero sul disco rigido *(per scopi di installazione)*

Requisiti hardware consigliati per **AVG AntiVirus**:

- CPU Intel Pentium da 1,8 GHz o superiore
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) di memoria RAM
- 1,6 GB di spazio libero sul disco rigido *(per scopi di installazione)*

3. Processo di installazione di AVG

Per installare **AVG AntiVirus** nel computer è necessario disporre del file di installazione più recente. Per assicurarsi di installare la versione aggiornata di **AVG AntiVirus**, si consiglia di scaricare il file di installazione dal sito Web di AVG (http://www.avg.com/). La sezione ***Centro di assistenza*** fornisce una panoramica strutturata dei file di installazione per ciascuna edizione di AVG. Dopo aver scaricato e salvato il file di installazione sul disco rigido, è possibile avviare il processo di installazione. L'installazione è una sequenza di finestre di dialogo semplici e chiare. Ciascuna finestra di dialogo descrive brevemente come procedere in ciascuna fase del processo di installazione. Di seguito viene fornita una descrizione dettagliata di ciascuna finestra di dialogo:

3.1. Finestra introduttiva

Il processo di installazione comincia con la finestra di dialogo ***Benvenuti in AVG Internet Security***:

Selezione lingua

In questa finestra di dialogo è possibile selezionare la lingua utilizzata per il processo di installazione. Fare clic sulla casella combinata accanto all'opzione ***Lingua*** per visualizzare il menu a discesa della lingua. Selezionare la lingua desiderata. Il processo di installazione procederà quindi nella lingua prescelta. Anche l'applicazione comunicherà nella lingua selezionata, con la possibilità di passare all'inglese (opzione installata per impostazione predefinita).

Contratto di licenza con l'utente finale e Informativa sulla privacy

Prima di proseguire con il processo di installazione, si consiglia di leggere il ***Contratto di licenza con l'utente finale*** e l'***Informativa sulla privacy***. È possibile accedere a entrambi i documenti tramite i collegamenti disponibili nella parte inferiore della finestra di dialogo. Fare clic su uno dei collegamenti ipertestuali per aprire

una nuova finestra di dialogo / finestra del browser dove è disponibile il testo completo del rispettivo documento. Si consiglia di leggere con attenzione questi documenti, poiché sono legalmente vincolanti. Fare clic sul pulsante ***Prosegui*** per confermare l'accettazione dei documenti.

Proseguire con l'installazione

Per proseguire con l'installazione, fare clic sul pulsante ***Prosegui***. Viene richiesto di indicare il License Number, quindi il processo di installazione procede in modalità completamente automatica. Alla maggior parte degli utenti si consiglia di mantenere selezionata l'opzione per l'installazione standard di **AVG AntiVirus** con tutte le impostazioni predefinite dal produttore del software. Questa configurazione fornisce la massima protezione combinata con l'utilizzo ottimale delle risorse. In futuro, se ci fosse necessità di modificare la configurazione, sarà possibile farlo direttamente nell'applicazione.

In alternativa è possibile scegliere l'opzione ***Installazione personalizzata***, utilizzando il collegamento ipertestuale disponibile sotto al pulsante ***Prosegui***. L'installazione personalizzata deve essere utilizzata solo da utenti esperti che hanno valide ragioni per installare l'applicazione con impostazioni non standard, ad esempio per soddisfare requisiti di sistema specifici. Se si decide di utilizzare questo tipo di installazione, immettere il License Number per visualizzare la finestra di dialogo ***Personalizza l'installazione***, dove è possibile specificare le impostazioni desiderate.

3.2. Immettere il License Number

Nella finestra di dialogo ***Attiva la licenza*** viene richiesto di immettere il License Number nell'apposito campo di testo:

Dove è possibile reperire il License Number

Il Sales Number si trova sulla custodia del CD nella confezione di **AVG AntiVirus** . Il License Number viene

comunicato nel messaggio email di conferma ricevuto dopo l'acquisto online di **AVG AntiVirus**. È necessario digitare il numero esattamente come viene indicato. Se il License Number è disponibile nel formato digitale (*contenuto nel messaggio email*), si consiglia di utilizzare il metodo "copia e incolla" per immetterlo.

Come utilizzare il metodo "copia e incolla"

L'uso del metodo ***copia e incolla*** per immettere il License Number di **AVG AntiVirus** nel programma assicura un'immissione corretta. Procedere come segue:

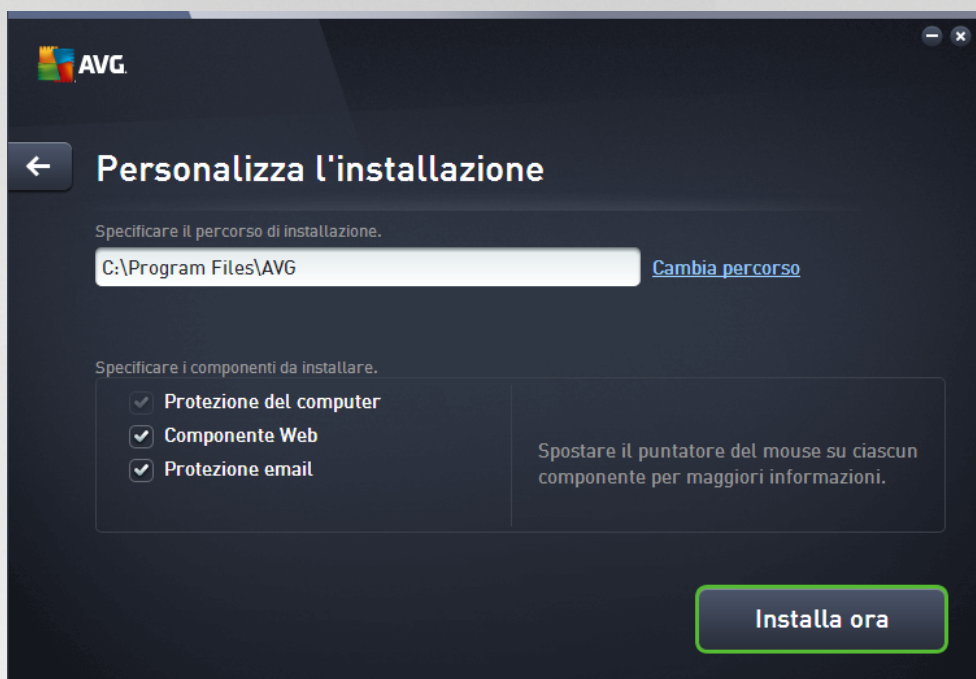
- Aprire il messaggio email che contiene il License Number.
- Posizionare il cursore all'inizio del License Number, premere il pulsante sinistro del mouse e, mantenendolo premuto, fare scorrere il cursore fino alla fine del numero, quindi rilasciare il pulsante. Il numero viene evidenziato.
- Tenendo premuto il tasto ***CTRL***, premere ***C***. Questa operazione copia il numero.
- Fare clic nella posizione in cui si desidera incollare il numero copiato.
- Tenendo premuto il tasto ***CTRL***, premere ***V***. Questa operazione incolla il numero nella posizione selezionata.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire dal processo di installazione. **AVG AntiVirus** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo dell'installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo dell'installazione.

3.3. Personalizzazione dell'installazione

La finestra di dialogo ***Opzioni personalizzate*** consente di impostare parametri di installazione dettagliati:

La sezione ***Selezione componenti*** offre una panoramica di tutti i componenti di **AVG AntiVirus** che è possibile installare. Se le impostazioni predefinite non sono adeguate alle proprie esigenze, è possibile rimuovere/aggiungere componenti specifici. ***È tuttavia possibile eseguire la selezione solo tra i componenti inclusi nell'edizione di AVG che è stata acquistata.*** Evidenziare una voce dell'elenco ***Selezione componenti*** per visualizzare una breve descrizione del relativo componente nella parte destra della sezione. Per informazioni dettagliate sulla funzionalità di ciascun componente, consultare il capitolo Panoramica dei componenti di questo documento. Per ripristinare la configurazione preimpostata dal fornitore del software, utilizzare il pulsante ***Predefinita***.

In questo passaggio è inoltre possibile decidere di installare varianti di lingua diverse da quelle predefinite nel prodotto *(per impostazione predefinita, l'applicazione viene installata nella lingua scelta per l'installazione e in inglese)*.

Pulsanti di controllo

Come avviene per la maggior parte delle finestre di dialogo, sono disponibili tre pulsanti di controllo:

- ***Annulla***: fare clic per uscire dal processo di installazione. **AVG AntiVirus** non verrà installato.
- ***Indietro***: fare clic per tornare alla precedente finestra di dialogo dell'installazione.
- ***Avanti***: fare clic per procedere con la successiva finestra di dialogo dell'installazione.

3.4. Installazione di AVG

Nella finestra di dialogo ***Avanzamento dell'installazione*** viene visualizzato l'avanzamento del processo di installazione. Non è necessario alcun intervento da parte dell'utente:

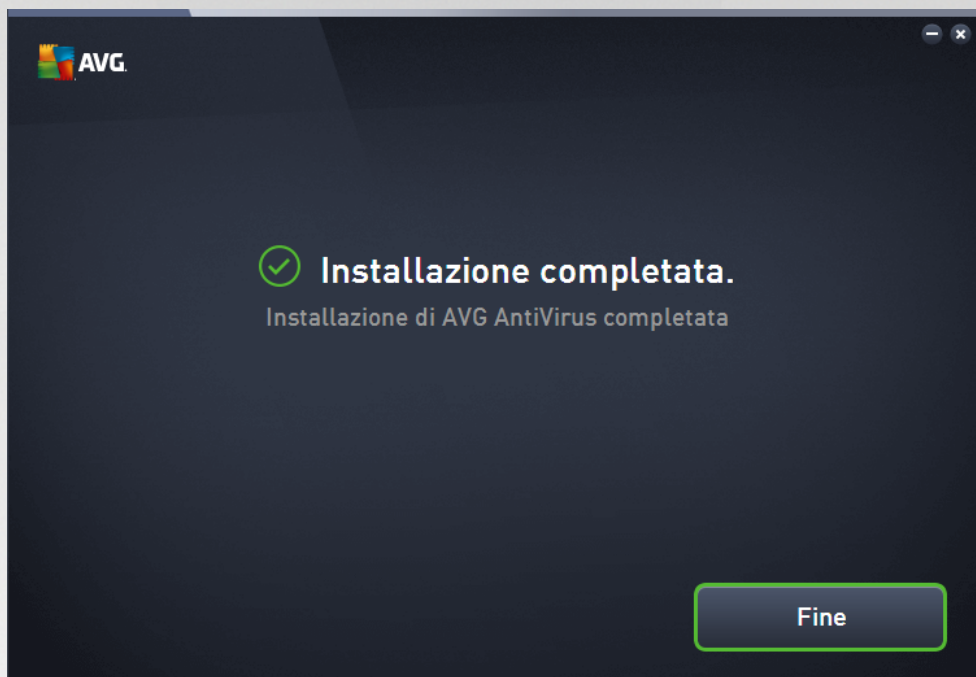
Al termine dell'installazione, si verrà reindirizzati automaticamente alla seguente finestra di dialogo.

Pulsanti di controllo

In questa finestra di dialogo sono disponibili due pulsanti di controllo:

- ***Riduci a icona***: il processo di installazione potrebbe richiedere alcuni minuti. Fare clic sul pulsante per ridurre la finestra di dialogo a icona sulla barra di sistema. La finestra di dialogo viene nuovamente visualizzata dopo aver completato l'installazione.
- ***Annulla***: questo pulsante deve essere utilizzato solo se si desidera arrestare il processo di installazione in corso. In tal caso **AVG AntiVirus** non verrà installato.

3.5. Installazione completata

La finestra di dialogo ***Congratulazioni*** conferma che **AVG AntiVirus** è stato installato e configurato correttamente:

Programma di miglioramento del prodotto e Informativa sulla privacy

Permette di decidere se partecipare al ***Programma di miglioramento del prodotto*** (*per dettagli, vedere il capitolo Impostazioni avanzate di AVG / Programma di miglioramento del prodotto*) che raccoglie informazioni anonime sulle minacce rilevate per aumentare il livello globale di protezione in Internet. Tutti i dati sono considerati riservati e in conformità all'Informativa sulla privacy di AVG. Fare clic sul collegamento ***Informativa sulla privacy*** per essere reindirizzati al sito Web di AVG (http://www.avg.com/) dove è possibile consultare il testo completo dell'Informativa sulla privacy di AVG. Se si accetta, mantenere l'opzione selezionata *(l'opzione viene confermata per impostazione predefinita)*.

Per completare l'installazione, fare clic sul pulsante ***Fine***.

4. Dopo l'installazione

4.1. Aggiornamento del database dei virus

Tenere presente che, al momento dell'installazione *(dopo il riavvio del computer, se necessario)*, **AVG AntiVirus** aggiorna automaticamente il database dei virus e tutti i componenti e li rende completamente operativi. Questa operazione può richiedere alcuni minuti. Mentre è in corso il processo di installazione, si riceverà una notifica dalle informazioni visualizzate nella finestra di dialogo principale. Al termine del processo di aggiornamento, la protezione di **AVG AntiVirus** sarà completamente attiva e funzionante.

4.2. Registrazione del prodotto

Al termine dell'installazione di **AVG AntiVirus**, registrare il prodotto in linea nel sito Web di AVG (*http://www.avg.com/*). Dopo la registrazione sarà possibile ottenere l'accesso completo all'account utente AVG, alla newsletter di aggiornamento AVG e ad altri servizi offerti esclusivamente agli utenti registrati. Il modo più facile per effettuare la registrazione è quello di procedere direttamente dall'interfaccia utente di **AVG AntiVirus**. Nel menu di spostamento superiore, selezionare la voce Opzioni / Registra ora. Si verrà reindirizzati alla pagina della ***registrazione*** del sito Web di AVG (*http://www.avg.com/*). Seguire le istruzioni fornite nella pagina.

4.3. Accesso all'interfaccia utente

È possibile accedere alla finestra di dialogo principale di AVG in diversi modi:

- tramite doppio clic sull'icona di AVG sulla barra delle applicazioni
- tramite doppio clic sull'icona di AVG sul desktop
- dal menu ***Start / Tutti i programmi / AVG / AVG Protection***

4.4. Scansione dell'intero computer

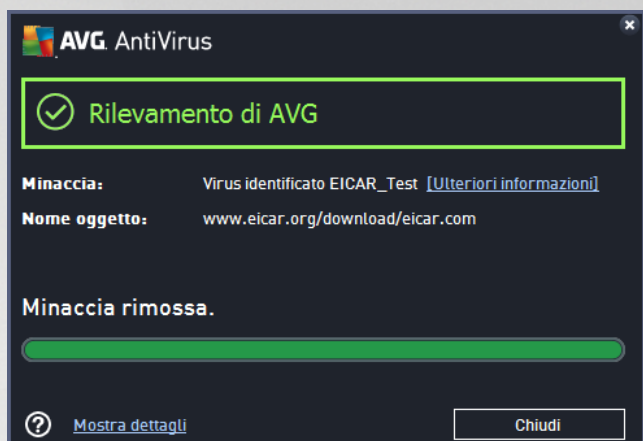
Esiste il rischio potenziale che un virus sia stato trasmesso al computer dell'utente prima dell'installazione di **AVG AntiVirus**. Per questo motivo è necessario eseguire Scansione intero computer per assicurarsi che non siano presenti infezioni sul PC. La prima scansione potrebbe richiedere diverso tempo *(circa un'ora)*, ma si consiglia di eseguirla comunque per verificare che il computer non sia stato compromesso da una minaccia. Per istruzioni sull'esecuzione di Scansione intero computer, consultare il capitolo Scansione AVG.

4.5. Controllo EICAR

Per confermare che **AVG AntiVirus** è stato installato correttamente è possibile eseguire il controllo EICAR.

Il controllo EICAR è un metodo standard e assolutamente sicuro per verificare il funzionamento del sistema antivirus. La sua esecuzione è sicura poiché non si tratta di un vero virus e non include frammenti di codice virale. La maggior parte dei prodotti vi reagisce come se si trattasse di un virus, *anche se normalmente lo segnala con un nome ovvio come "EICAR-AV-Test"*. È possibile scaricare il virus EICAR dal sito Web di EICAR all'indirizzo www.eicar.com, in cui si troveranno anche tutte le informazioni necessarie sul controllo EICAR.

Provare a scaricare il file *eicar.com* e a salvarlo sul disco locale. Subito dopo aver confermato il download del

file di controllo, **AVG AntiVirus** visualizzerà un avviso. Questo avviso dimostra che AVG è stato installato correttamente nel computer.

Se AVG non identifica il file di controllo EICAR come un virus, è necessario verificare nuovamente la configurazione del programma.

4.6. Configurazione predefinita di AVG

La configurazione predefinita (*ovvero la modalità di impostazione dell'applicazione dopo l'installazione*) di **AVG AntiVirus** è impostata dal fornitore del software in modo che tutti i componenti e le funzioni siano ottimizzati per offrire il massimo delle prestazioni. ***A meno che non esista un motivo valido per farlo, si consiglia di non modificare la configurazione di AVG! Le modifiche alle impostazioni dovrebbero essere eseguite solo da un utente esperto.*** Se si desidera modificare la configurazione di AVG per adeguare l'applicazione alle proprie esigenze, accedere a Impostazioni AVG avanzate: selezionare la voce del menu principale *Opzioni/Impostazioni avanzate* e modificare la configurazione di AVG nella finestra di dialogo Impostazioni AVG avanzate visualizzata.

5. Interfaccia utente di AVG

AVG AntiVirus apre con la finestra principale:

La finestra principale è suddivisa in diverse sezioni:

- ***Menu di spostamento superiore***: include i quattro collegamenti attivi allineati nella parte superiore della finestra principale *(Ti piace AVG?, Rapporti, Supporto, Opzioni)*. Dettagli >>
- ***Informazioni sullo stato di protezione***: fornisce informazioni di base sullo stato corrente di **AVG AntiVirus**. Dettagli >>
- ***Panoramica dei componenti installati***: facendo clic sui riquadri al centro della finestra principale è possibile accedere ai vari componenti. I componenti vengono visualizzati come blocchi di colore verde chiaro, contrassegnati dalle rispettive icone e informazioni sullo stato. Dettagli >>
- ***Applicazioni personali***: visualizzate graficamente nella striscia centrale inferiore della finestra principale, offrono una panoramica delle applicazioni complementari ad **AVG AntiVirus** già installate nel computer o che è consigliabile installare. Dettagli >>
- ***Collegamenti rapidi per la scansione, la correzione e l'aggiornamento***: sono posizionati nella riga di blocchi inferiore della finestra principale. Questi pulsanti consentono un accesso immediato alle funzionalità più importanti e più utilizzate di AVG. Dettagli >>

Oltre alla finestra principale di **AVG AntiVirus** è presente un altro elemento di controllo che consente di accedere all'applicazione:

- L'***icona nell'area di notifica***, posizionata *sulla barra delle applicazioni* nell'angolo inferiore destro dello schermo, indica lo stato corrente di **AVG AntiVirus**. Dettagli >>

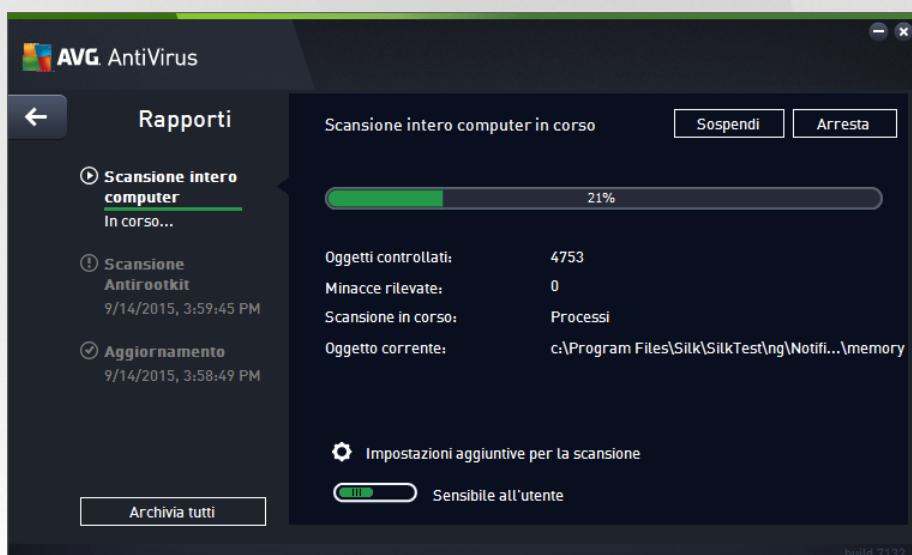
5.1. Menu di spostamento superiore

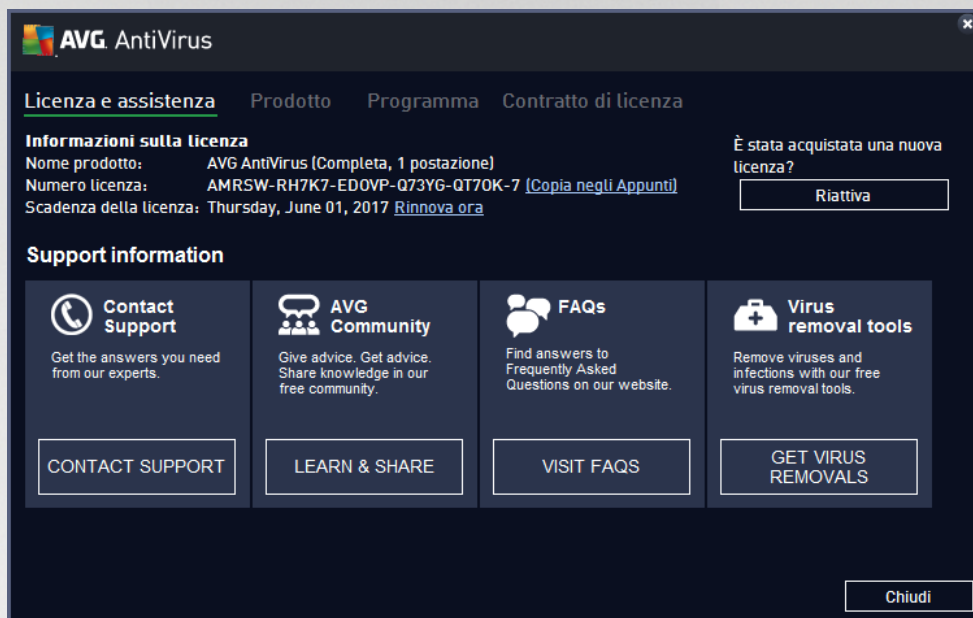
Nel ***menu di spostamento superiore*** sono presenti diversi collegamenti attivi allineati nella parte superiore della finestra principale. Il menu di spostamento include i seguenti pulsanti:

5.1.1. AVG su Facebook

Fare clic sul collegamento per connettersi alla comunità Facebook di AVG e condividere informazioni, novità e suggerimenti di AVG per la massima protezione di Internet.

5.1.2. Rapporti

Consente di aprire una nuova finestra di dialogo ***Rapporti*** con una panoramica di tutti i rapporti relativi alla scansioni avviate in precedenza e ai processi aggiornati. Se la scansione o l'aggiornamento è attualmente in esecuzione, verrà visualizzata un'icona rotante accanto al testo ***Rapporti*** nel menu di esplorazione superiore dell'interfaccia utente principale. Fare clic su tale icona per visualizzare nella finestra di dialogo l'avanzamento del processo in esecuzione:

5.1.3. Assistenza

Apre una nuova finestra di dialogo composta da quattro schede in cui è possibile trovare tutte le informazioni rilevanti su **AVG AntiVirus**:

- ***Licenza e assistenza***: questa scheda fornisce le informazioni relative a nome prodotto, License Number e data di scadenza. Nella parte inferiore della finestra di dialogo è inoltre presente una panoramica organizzata in modo chiaro di tutti i contatti disponibili per l'assistenza clienti. Nella scheda sono disponibili i seguenti pulsanti e collegamenti attivi:
  - *(Ri)attiva*: fare clic per aprire la nuova finestra di dialogo ***Attiva software AVG***. Immettere il License Number nell'apposito campo per sostituire il Sales Number *(utilizzato per l'installazione di AVG AntiVirus)* oppure per cambiare il License Number corrente con un altro *(ad esempio, in caso di upgrade a un prodotto AVG più avanzato)*.
  - *Copia negli Appunti*: utilizzare questo collegamento per copiare il License Number e incollarlo dove necessario. In questo modo si sarà certi di immettere il License Number corretto.
  - *Rinnova ora*: è consigliabile acquistare il rinnovo della licenza di **AVG AntiVirus** in anticipo, almeno un mese prima della scadenza della licenza corrente. L'utente verrà avvisato quando il periodo di licenza sta per scadere. Facendo clic su questo collegamento si viene reindirizzati al sito Web di AVG *(http://www.avg.com/)* dove è possibile trovare informazioni dettagliate sullo stato della licenza, la data di scadenza e l'offerta di rinnovo/upgrade.
- ***Prodotto***: questa scheda offre una panoramica dei dati tecnici più importanti di **AVG AntiVirus**, quali informazioni sul prodotto, sui componenti installati e sulla protezione email installata.
- ***Programma***: in questa scheda è possibile trovare informazioni sulla versione dei file di programma e sul codice di terzi utilizzato nel prodotto.
- ***Contratto di licenza***: in questa scheda è disponibile il testo completo del Contratto di licenza tra l'utente e AVG Technologies.

5.1.4. Opzioni

La manutenzione di **AVG AntiVirus** è accessibile tramite la voce ***Opzioni***. Fare clic sulla freccia per aprire il menu a discesa:

- ***Scansione computer*** avvia una scansione dell'intero computer.
- ***Scansione cartella selezionata...***: consente di passare all'interfaccia di scansione di AVG e di definire i file e le cartelle da sottoporre a scansione nella struttura del computer.
- ***Scansione file...***: consente di eseguire un controllo su richiesta di un singolo file specifico. Fare clic su questa opzione per aprire una nuova finestra con la struttura del disco. Selezionare il file desiderato e confermare l'avvio della scansione.
- ***Aggiorna***: avvia automaticamente il processo di aggiornamento di **AVG AntiVirus**.
- ***Aggiorna da directory...***: esegue il processo di aggiornamento dai file di aggiornamento che si trovano in una cartella specifica sul disco locale. Tuttavia, questa opzione è consigliabile solo in caso di emergenza, come in situazioni in cui non è disponibile la connessione a Internet (ad esempio, il computer è stato infettato e si è disconnesso da Internet, il computer è connesso a una rete senza accesso a Internet e così via). Nella finestra appena aperta selezionare la cartella in cui è stato precedentemente posizionato il file di aggiornamento e avviare il processo di aggiornamento.
- ***Quarantena virus***: consente di aprire l'interfaccia della finestra di quarantena (Quarantena virus) in cui AVG sposta tutte le infezioni rilevate. All'interno della quarantena i file infetti vengono isolati e la protezione del computer è garantita. Allo stesso tempo, i file infetti vengono archiviati per una possibile riparazione futura.
- ***Cronologia***: offre ulteriori opzioni specifiche nel sottomenu.
    - *Risultati scansione*: consente di aprire una finestra di dialogo con una panoramica dei risultati della scansione.
    - *Risultati di Resident Shield*: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Resident Shield.
    - *Risultati di Identity Protection*: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate dal componente Identity Protection.
    - *Risultati di Protezione email*: consente di aprire una finestra di dialogo con una panoramica degli allegati email rilevati come pericolosi dal componente Protezione email.
    - *Risultati di Online Shield*: consente di aprire una finestra di dialogo con una panoramica delle minacce rilevate da Online Shield.
    - *Log cronologia eventi*: consente di aprire l'interfaccia di Log cronologia con una panoramica di tutte le azioni di **AVG AntiVirus** registrate.
- ***Impostazioni avanzate...***: consente di aprire la finestra di dialogo delle impostazioni AVG avanzate in cui è possibile modificare la configurazione di **AVG AntiVirus**. In genere è consigliabile mantenere le impostazioni dell'applicazione predefinite dal fornitore del software.
- ***Sommario Guida***: consente di aprire i file della Guida di AVG.

- ***Ottieni assistenza***: consente di aprire la finestra di dialogo dell'assistenza, in cui sono disponibili tutti i contatti e le informazioni per l'assistenza.
- ***Web AVG personale***: consente di aprire il sito Web di AVG (*http://www.avg.com/*).
- ***Informazioni sui virus e le minacce***: consente di aprire l'enciclopedia dei virus online sul sito Web di AVG (*http://www.avg.com/*) in cui è possibile trovare informazioni dettagliate sul virus identificato.
- ***(Ri)attiva***: consente di aprire la finestra di dialogo di attivazione con il License Number fornito durante il processo di installazione. In questa finestra di dialogo è possibile modificare il License Number per sostituire il Sales Number (*il numero con cui è stata eseguita l'installazione di AVG*) o il License Number in uso (*ad esempio, durante l'upgrade a un nuovo prodotto AVG*). Se è in uso la versione di prova di **AVG AntiVirus**, le ultime due voci vengono visualizzate come ***Acquista ora*** e ***Attiva***, consentendo di acquistare subito la versione completa del programma. Se invece **AVG AntiVirus** è stato installato con un Sales Number, le voci vengono visualizzate come ***Registra*** e ***Attiva***:
- ***Registra ora / AVG MyAccount***: consente di connettersi alla pagina relativa alla registrazione del sito Web di AVG (*http://www.avg.com/*). Immettere i dati di registrazione. Solo i clienti che registrano il prodotto AVG possono ricevere assistenza tecnica gratuita.
- ***Informazioni su AVG***: consente di aprire una nuova finestra di dialogo con quattro schede in cui sono presenti i dati sul tipo di licenza acquistata e le informazioni disponibili sull'assistenza, il prodotto e il programma, oltre al testo completo del Contratto di licenza. *(In alternativa, è possibile accedere a questa finestra di dialogo utilizzando il collegamento Assistenza nella finestra principale.)*

5.2. Informazioni sullo stato della protezione

La sezione ***Impostazioni sullo stato di protezione*** si trova nella parte superiore della **AVG AntiVirus** finestra principale. All'interno di questa sezione sono contenute le informazioni sullo stato di protezione corrente di **AVG AntiVirus**. Qui di seguito è disponibile una panoramica delle possibili icone, con il relativo significato:

- l'icona verde indica che ***AVG AntiVirus è completamente funzionante***. Il computer è totalmente protetto, aggiornato e tutti i componenti installati funzionano correttamente.

- l'icona gialla indica ***la configurazione non corretta di uno o più componenti***. È consigliabile controllare le relative proprietà/impostazioni. Non sono presenti problemi gravi in **AVG AntiVirus** e probabilmente è stato deciso di disattivare un componente per qualche ragione. La protezione è comunque attiva. Tuttavia, prestare attenzione alle impostazioni del componente in cui si sono verificati problemi. Il componente configurato in modo errato verrà visualizzato con una striscia arancione di avviso nell'interfaccia utente principale.

L'icona gialla viene inoltre visualizzata se, per qualche motivo, l'utente ha deciso di ignorare lo stato di errore di un componente. L'opzione ***Ignora lo stato di errore*** è accessibile nel ramo Impostazioni avanzate / Ignora stato di errore. Qui è presente l'opzione per confermare che si è al corrente dello stato di errore del componente, tuttavia si desidera mantenere **AVG AntiVirus** nella condizione attuale e non si desidera ricevere notifiche a riguardo. Potrebbe essere necessario utilizzare l'opzione ***Ignora stato del componente*** in situazioni particolari, tuttavia si consiglia di disattivare questa opzione nel più breve tempo possibile.

In alternativa, l'icona gialla verrà visualizzata anche se **AVG AntiVirus** richiede il riavvio del computer (***Riavvio necessario***). Prestare attenzione all'avviso e riavviare il PC.

- l'icona arancione indica che ***AVG AntiVirus si trova in uno stato critico***. Uno o più componenti non funzionano correttamente e **AVG AntiVirus** non è in grado di proteggere il computer. Intervenire immediatamente per risolvere il problema segnalato! Se non si è in grado di correggere l'errore, contattare il team dell'Assistenza tecnica di AVG.

Se AVG AntiVirus non è impostato in modo da ottenere prestazioni ottimali, un nuovo pulsante denominato Risolvi problema (oppure Fare clic per risolvere i problemi, se sono interessati più componenti) appare accanto alle informazioni sullo stato di protezione. Selezionare il pulsante per avviare un processo automatico di controllo e configurazione del programma. Si tratta di un modo per impostare facilmente AVG AntiVirus per ottenere prestazioni ottimali e massima protezione.

Si consiglia di prestare attenzione alla sezione ***Informazioni sullo stato di protezione*** e, nel caso in cui fosse segnalato un problema, procedere cercando di risolverlo immediatamente. In caso contrario, il computer è a rischio.

Nota: *le informazioni sullo stato di AVG AntiVirus sono sempre disponibili anche tramite l'icona nell'area di notifica sulla barra delle applicazioni.*

5.3. Panoramica dei componenti

La ***panoramica dei componenti installati*** è disponibile nella sezione centrale della finestra principale. I componenti vengono visualizzati come blocchi di colore verde chiaro, contrassegnati dalle rispettive icone. Ogni blocco fornisce informazioni sullo stato corrente della protezione. Se il componente è stato configurato correttamente ed è completamente funzionante, l'informazione viene riportata in caratteri verdi. Se il componente viene arrestato e la relativa funzionalità viene limitata o se il componente si trova in stato di errore, l'utente verrà informato tramite un messaggio di avviso visualizzato in un campo di testo arancione. ***Si consiglia di controllare le impostazioni del componente.***

Spostare il puntatore sul componente per visualizzare un breve testo nella parte inferiore della finestra principale. Il testo fornisce un'introduzione di base alla funzionalità del componente. Comunica inoltre lo stato corrente del componente e specifica quali servizi del componente non sono configurati correttamente.

Elenco dei componenti installati

In **AVG AntiVirus** la sezione ***Panoramica dei componenti*** contiene informazioni sui seguenti componenti:

- ***Computer*** - questo componente comprende due servizi: ***AntiVirus Shield***, che rileva virus, spyware, worm, trojan, librerie o file eseguibili indesiderati presenti nel sistema e protegge da adware dannoso, ed ***Anti-Rootkit***, in grado di ricercare i rootkit pericolosi nascosti in applicazioni, driver o librerie. Dettagli >>

- ***Web*** - assicura la protezione dagli attacchi basati sul Web durante le ricerche e l'esplorazione online. Dettagli >>

- ***Identità*** - Questo componente esegue il servizio ***Identity Shield*** che assicura la protezione costante delle risorse digitali contro le nuove minacce online. Dettagli >>

- ***Email*** - controlla la presenza di SPAM nei messaggi email in arrivo e blocca virus, attacchi di phishing o altre minacce. Dettagli >>

Azioni accessibili

- ***Posizionare il mouse sull'icona di un componente*** per evidenziarlo all'interno della panoramica dei componenti. Nella parte inferiore dell'interfaccia utente viene inoltre visualizzata la descrizione delle funzionalità di base del componente.

- ***Fare clic sull'icona del componente*** per aprire l'interfaccia con le informazioni relative allo stato corrente e accedere alla configurazione e ai dati statistici del componente.

5.4. Applicazioni personali

Nell'area ***Applicazioni personali*** *(la riga di blocchi verdi sotto il gruppo dei componenti)* è possibile trovare una panoramica di ulteriori applicazioni di AVG che sono pronte per essere installate sul computer o che si consiglia di installare. I blocchi vengono visualizzati in modo condizionale e possono rappresentare una delle seguenti applicazioni:

- ***Protezione mobile*** è un'applicazione che protegge il cellulare da virus e malware. Fornisce inoltre la capacità di rilevare lo smartphone in modalità remota in caso di necessità.

- ***LiveKive*** è destinato al backup dei dati online su server sicuri. LiveKive esegue il backup automatico di tutti i file, le foto e la musica in una posizione sicura, consentendo di condividerli con familiari e amici e di accedervi da qualsiasi dispositivo abilitato per il Web, inclusi dispositivi Android e iPhone.

- ***Family Safety*** aiuta a proteggere i bambini da siti Web, ricerche online e contenuti multimediali inappropriati e fornisce rapporti delle attività online dei bambini che utilizzano il computer. AVG Family Safety utilizza tecnologie di monitoraggio della pressione dei tasti per controllare le attività dei bambini nelle chat room e nei social network. Se vengono rilevati termini o espressioni tipicamente utilizzati per adescare i bambini online, il programma invia immediatamente una notifica ai genitori tramite SMS o email. L'applicazione consente di impostare il livello di protezione che meglio si adatta a ciascun bambino e controllarne l'attività separatamente tramite dati di accesso univoci.

- L'applicazione ***PC TuneUp*** è uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni generali del computer.

- ***AVG Toolbar*** è disponibile direttamente nel browser Internet per assicurare la protezione massima durante l'esplorazione in Internet.

Per informazioni dettagliate sulle applicazioni di ***Applicazioni personali*** fare clic sul relativo blocco. Si verrà reindirizzati alla pagina Web di AVG dedicata, da cui è possibile scaricare immediatamente il componente.

5.5. Collegamenti rapidi Scansione / Aggiornamento

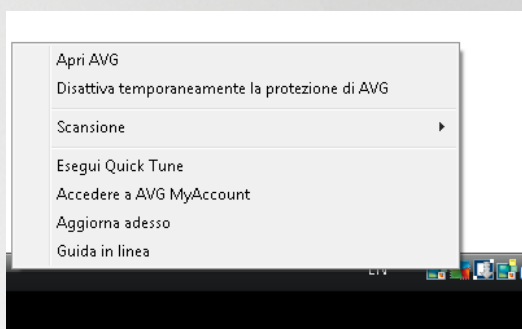
I collegamenti rapidi sono disponibili nella fila inferiore di pulsanti nell'interfaccia utente di **AVG AntiVirus**. Questi collegamenti consentono di accedere immediatamente alle funzionalità più importanti e più utilizzate dell'applicazione, ovvero scansione e aggiornamento. I collegamenti rapidi sono accessibili da tutte le finestre di dialogo dell'interfaccia utente:

- ***Esegui scansione***: questo pulsante è diviso graficamente in due sezioni. Selezionare il collegamento ***Esegui scansione*** per avviare la Scansione intero computer e visualizzare l'avanzamento e i relativi risultati nella finestra Rapporti, che viene aperta automaticamente. Il pulsante ***Opzioni*** apre la finestra di dialogo ***Opzioni di scansione*** in cui è possibile gestire le scansioni pianificate e modificare i

parametri di Scansione intero computer / Scansione file o cartelle. *Per informazioni dettagliate, vedere il capitolo Scansione AVG.*

- ***Ottimizza le prestazioni**:* questo pulsante consente di accedere al servizio ***PC Analyzer***, uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che permette di migliorare la velocità e le prestazioni complessive del computer.
- ***Aggiorna adesso***: premere questo pulsante per avviare subito l'aggiornamento del prodotto. L'utente verrà informato dei risultati dell'aggiornamento nel riquadro sopra l'icona di AVG nell'area di notifica sulla barra delle applicazioni. *Per informazioni dettagliate, vedere il capitolo Aggiornamenti di AVG.*

5.6. Icona nell'area di notifica della barra delle applicazioni

L'***icona di AVG nell'area di notifica*** *(presente sulla barra delle applicazioni di Windows, nell'angolo inferiore destro dello schermo)* indica lo stato corrente di **AVG AntiVirus**. È sempre disponibile sulla barra delle applicazioni, indipendentemente dall'apertura o meno dell'interfaccia utente di **AVG AntiVirus**:

Aspetto dell'icona di AVG nell'area di notifica sulla barra delle applicazioni

- Se è completamente colorata e non presenta elementi aggiuntivi, l'icona indica che tutti i componenti di **AVG AntiVirus** sono attivi e funzionano correttamente. Tuttavia, l'icona può venire visualizzata in questo modo anche quando uno dei componenti non è completamente funzionante ma l'utente ha deciso di ignorare lo stato di quel componente. *Selezionando l'opzione Ignora stato del componente si conferma di essere al corrente dello stato di errore del componente, tuttavia si desidera mantenere la condizione attuale e non si desidera ricevere notifiche a riguardo.*
- L'icona con un punto esclamativo indica che uno *o più componenti* si trovano in uno stato di errore. Prestare sempre attenzione a tale avviso e tentare di risolvere il problema di configurazione del componente non impostato correttamente. Per modificare la configurazione del componente, fare doppio clic sull'icona nell'area di notifica sulla barra delle applicazioni per aprire l'interfaccia utente dell'applicazione. Per informazioni dettagliate sui componenti in stato di errore, vedere la sezione relativa alle informazioni sullo stato di protezione.
- L'icona nell'area di notifica sulla barra delle applicazioni può essere inoltre visualizzata completamente colorata con un fascio di luce rotante. Questa versione segnala che è in corso un processo di aggiornamento.
- La visualizzazione alternativa dell'icona completamente colorata con una freccia centrale indica che è in esecuzione una scansione di **AVG AntiVirus**.

Informazioni sull'icona di AVG nell'area di notifica sulla barra delle applicazioni

L'***icona di AVG nell'area di notifica sulla barra delle applicazioni*** fornisce inoltre informazioni sulle attività correnti di **AVG AntiVirus**, ed eventuali modifiche dello stato del programma (*ad esempio, avvio automatico di una scansione o un aggiornamento pianificato, modifica dello stato di un componente, presenza di uno stato di errore e così via*) tramite una finestra a comparsa che si apre dall'icona stessa.

Azioni accessibili tramite l'icona di AVG nell'area di notifica sulla barra delle applicazioni

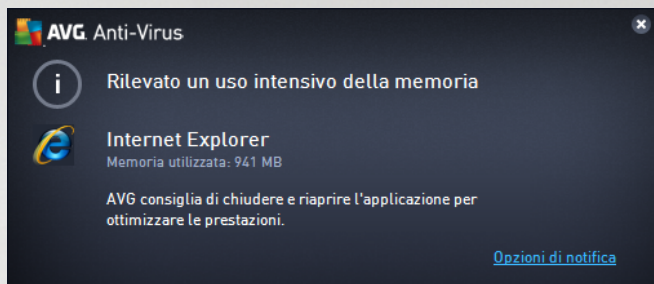
L'***icona di AVG nell'area di notifica sulla barra delle applicazioni*** può inoltre essere utilizzata come collegamento rapido per accedere all'interfaccia utente di **AVG AntiVirus**, semplicemente tramite doppio clic. Se si fa clic con il pulsante destro del mouse sull'icona, viene aperto un menu di scelta rapida contenente le seguenti opzioni:

- ***Apri AVG***: fare clic per aprire l'interfaccia utente di **AVG AntiVirus**.
- ***Disattiva temporaneamente la protezione di AVG***: questa opzione consente di disattivare completamente la protezione assicurata da **AVG AntiVirus**. Non utilizzare questa opzione se non è assolutamente necessario. Nella maggior parte dei casi, non è necessario disattivare **AVG AntiVirus** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. Se fosse necessario disattivare temporaneamente **AVG AntiVirus**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.
- ***Scansione***: fare clic per aprire il menu di scelta rapida delle scansioni predefinite (*Scansione intero computer* e *Scansione file o cartelle*) e selezionare la scansione richiesta, che verrà avviata immediatamente.
- ***Esecuzione delle scansioni in corso***: questa voce viene visualizzata solo se nel computer è in esecuzione una scansione. Per questa scansione è possibile impostare la priorità oppure arrestarla o sospenderla. Sono inoltre accessibili le seguenti azioni: *Imposta priorità per tutte le scansioni, Sospendi tutte le scansioni* o *Arresta tutte le scansioni*.
- ***Ottimizza le prestazioni***: fare clic per avviare il componente PC Analyzer.
- ***Accedi ad AVG MyAccount***: apre la pagina iniziale di AVG MyAccount in cui è possibile gestire i prodotti in abbonamento, acquistare protezione aggiuntiva, scaricare i file di installazione, controllare gli ordini e le fatture precedenti e gestire le informazioni personali.
- ***Aggiorna adesso***: viene avviato un aggiornamento immediato.
- ***Guida in linea***: apre il file della Guida alla pagina iniziale.

5.7. AVG Advisor

AVG Advisor è stato progettato per rilevare i problemi che potrebbero causare un rallentamento o mettere a rischio la protezione del computer e per suggerire una soluzione. Se si verifica un improvviso rallentamento del computer *(esplorazione di Internet, prestazioni complessive)*, generalmente non è facile capire quale sia la

causa del problema e quindi come risolverlo. In questi casi ***AVG Advisor*** visualizza una notifica sulla barra delle applicazioni che segnala il possibile problema e suggerisce come risolverlo. ***AVG Advisor*** tiene costantemente sotto controllo tutti i processi in esecuzione nel PC, offrendo suggerimenti utili per evitare eventuali problemi.

Le ***notifiche di AVG Advisor*** vengono visualizzate sotto forma di finestra a comparsa sulla barra delle applicazioni:

In particolare, ***AVG Advisor*** monitora i seguenti elementi:

- ***Lo stato dei browser Web attualmente aperti***. I browser Web possono sovraccaricare la memoria, in particolare se si lasciano aperte per diverso tempo più schede o finestre, e utilizzare una quantità eccessiva di risorse di sistema, rallentando il computer. In tali situazioni, in genere è consigliabile riavviare il browser Web.

- ***Esecuzione di connessioni peer-to-peer***. Dopo l'utilizzo del protocollo P2P per la condivisione di file, talvolta la connessione può rimanere attiva impegnando una certa quantità di larghezza di banda. Di conseguenza, può verificarsi un rallentamento dell'esplorazione Web.

- ***Reti sconosciute con un nome familiare***. Questa situazione in genere si applica solo agli utenti che si connettono a più reti, solitamente con computer portatili. Se una nuova rete sconosciuta ha lo stesso nome di una rete nota e utilizzata di frequente, *ad esempio Casa o Wi-Fi,*, l'utente potrebbe collegarsi accidentalmente a una rete completamente sconosciuta e potenzialmente non sicura. ***AVG Advisor*** può impedire questa situazione segnalando che la rete apparentemente nota è in realtà una nuova rete. Se si decide che la nuova rete è sicura, è possibile salvarla nell'elenco delle reti note di ***AVG Advisor*** , in modo che non venga più segnalata in seguito.

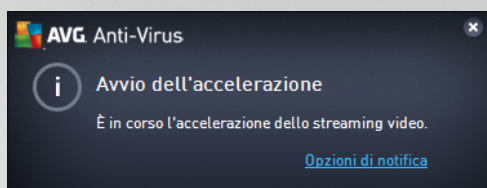
In tutti questi casi, ***AVG Advisor*** comunica la presenza di possibili problemi e fornisce il nome e l'icona del processo o dell'applicazione in conflitto. Inoltre, ***AVG Advisor*** suggerisce la procedura da eseguire per evitare i possibili problemi.

Browser Web supportati

La funzionalità è compatibile con i seguenti browser Web: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. AVG Accelerator

AVG Accelerator ottimizza la riproduzione dei video online e semplifica il download. Quando il processo di accelerazione video è in corso, l'utente ne verrà informato tramite la finestra a comparsa sulla barra delle applicazioni.

AVG Anti-Virus
Avvio dell'accelerazione
È in corso l'accelerazione dello streaming video.
Opzioni di notifica

6. Componenti di AVG

6.1. Protezione del computer

Il componente ***Computer*** comprende due servizi di protezione principali: ***AntiVirus*** e ***Archivio dati protetto***.

- ***AntiVirus*** è costituito da un motore di scansione che controlla tutti i file, le aree di sistema del computer e i supporti rimovibili *(unità flash e così via)* e ricerca i virus noti. Tutti i virus rilevati vengono bloccati per essere poi corretti o messi in Quarantena virus. Questo processo non viene notato dall'utente, poiché la protezione permanente viene eseguita "in background". AntiVirus utilizza anche la scansione euristica, che consente di rilevare le caratteristiche tipiche dei virus. In questo modo AntiVirus è in grado di rilevare un nuovo virus sconosciuto, se tale virus contiene alcune caratteristiche tipiche dei virus esistenti. **AVG AntiVirus** è inoltre in grado di analizzare e rilevare le applicazioni eseguibili o le librerie DLL che potrebbero essere potenzialmente indesiderate nel sistema *(vari tipi di spyware, adware e così via)*. Inoltre, AntiVirus esegue la scansione del Registro di sistema alla ricerca di voci sospette e file Internet temporanei e consente di trattare tutti gli elementi potenzialmente indesiderati come avviene per le altre infezioni.

- ***Archivio dati protetto*** consente di creare archivi virtuali protetti per archiviare dati sensibili o importanti. Il contenuto di un archivio dati protetto viene crittografato e protetto con una password definita dall'utente, in modo da renderlo inaccessibile a chi non dispone dall'autorizzazione.

Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del pannello relativo al servizio desiderato. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo sono disponibili i seguenti controlli. Il funzionamento è identico, indipendentemente dal servizio di protezione a cui appartengono *(AntiVirus o Archivio dati protetto)*:

Attivato / Disattivato: questo pulsante è simile a un semaforo, sia nell'aspetto che nella

funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde rappresenta lo stato ***Attivato***, ovvero indica che il servizio di protezione AntiVirus è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato***, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se è necessario disattivare il servizio, per mettere in guardia dai possibili rischi viene visualizzato il segnale rosso di ***Avviso*** con la notifica che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero AntiVirus. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione incluso in **AVG AntiVirus**, tuttavia si sconsiglia agli utenti meno esperti di apportare modifiche.

Freccia: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'interfaccia utente principale.

Come creare un archivio dati protetto

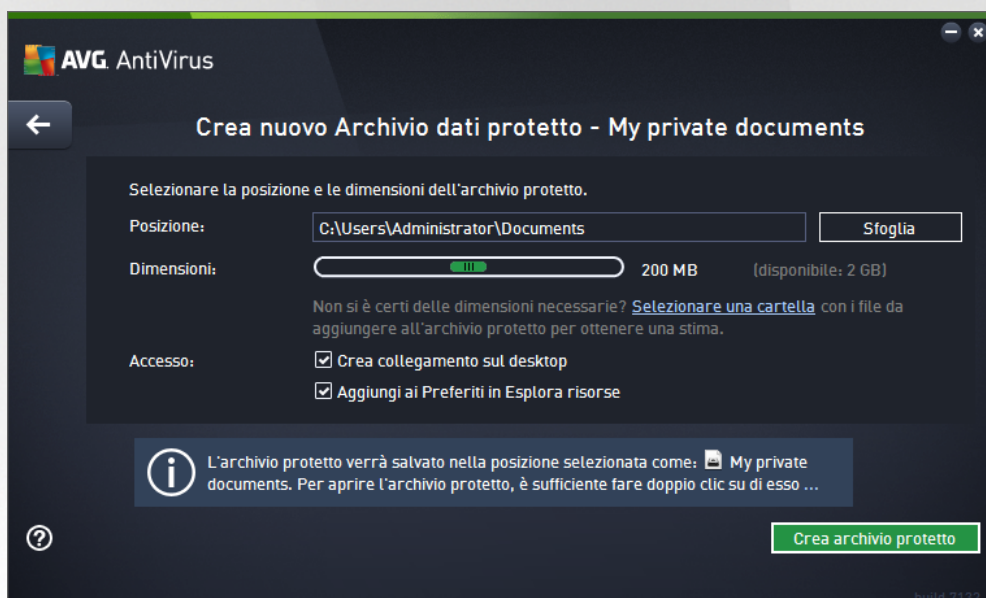
Nella sezione ***Archivio dati protetto*** della finestra di dialogo ***Protezione del computer*** è disponibile il pulsante ***Crea archivio protetto***. Fare clic sul pulsante per aprire una nuova finestra di dialogo con lo stesso nome in cui è possibile specificare i parametri dell'archivio protetto da creare. Immettere le informazioni necessarie e seguire le istruzioni nell'applicazione:

Innanzitutto è necessario specificare il nome dell'archivio protetto e creare una password complessa:

- ***Nome archivio dati protetto***: per creare un nuovo archivio protetto, è innanzitutto necessario scegliere un nome appropriato per riconoscerlo. Se si condivide il computer con altri familiari, è consigliabile includere il proprio nome oltre all'indicazione del contenuto dell'archivio, ad esempio *Email di papà*.

- ***Creare la password / Ridigitare la password***: creare una password per l'archivio dati protetto e digitarla nei rispettivi campi di testo. L'indicatore grafico a destra segnala se la password dell'utente è vulnerabile *(relativamente facile da identificare con speciali strumenti software)* o complessa. È consigliabile scegliere una password di complessità almeno media. È possibile rendere più sicura la password aggiungendo lettere maiuscole, numeri e altri caratteri come punti, trattini e così via. Per essere certi che la password sia stata digitata nel modo desiderato, è possibile selezionare la casella ***Mostra password*** *(ovviamente è necessario assicurarsi che nessuno stia guardando lo schermo)*.

- ***Suggerimento password***: è consigliabile creare anche un suggerimento utile per ricordare la password in caso di necessità. Tenere presente che un archivio dati protetto viene creato per proteggere i file consentendo l'accesso solo con la password. Non è possibile eludere la protezione e se si dimentica la password non sarà possibile accedere all'archivio dati protetto.

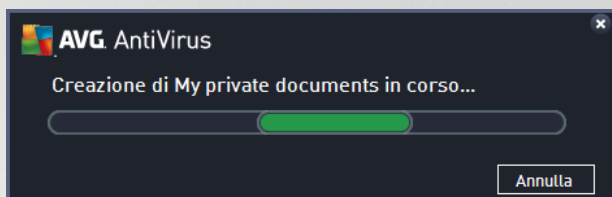
Dopo aver specificato nei campi di testo tutti i dati richiesti, fare clic sul pulsante ***Avanti*** per procedere al passaggio successivo:

Questa finestra di dialogo fornisce le seguenti opzioni di configurazione:

- ***Posizione***: indica dove verrà collocato fisicamente l'archivio protetto. Individuare una destinazione appropriata nel disco rigido oppure mantenere la posizione predefinita, ovvero la cartella *Documenti*. Tenere presente che dopo aver creato un archivio dati protetto non è possibile modificarne la posizione.

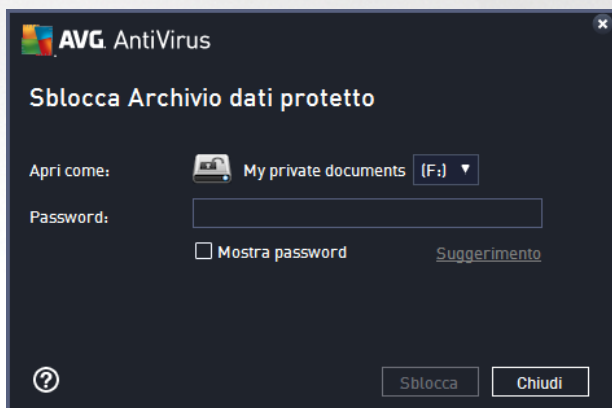
- ***Dimensioni***: è possibile impostare le dimensioni predefinite dell'archivio dati protetto, in modo da allocare lo spazio necessario su disco. Il valore impostato non deve essere troppo piccolo *(insufficiente per le esigenze dell'utente)*, né troppo grande *(tale da occupare troppo spazio su disco inutilmente)*. Se è già stato deciso cosa trasferire nell'archivio dati protetto, è possibile inserire tutti i file in una cartella e utilizzare il collegamento ***Selezionare una cartella*** per calcolare automaticamente le dimensioni totali. È comunque possibile modificare le dimensioni in un secondo momento in base alle esigenze.

- ***Accesso***: le caselle di controllo presenti in questa sezione consentono di creare collegamenti rapidi all'archivio dati protetto.

Come utilizzare l'archivio dati protetto

Dopo aver configurato le impostazioni desiderate, fare clic sul pulsante ***Crea archivio protetto***. Verrà visualizzata una nuova finestra di dialogo ***L'archivio dati è pronto*** che indica che l'archivio dati è pronto per l'archiviazione dei file. L'archivio dati è ora aperto ed è possibile accedervi immediatamente. In seguito, per accedere nuovamente all'archivio dati sarà necessario sbloccarlo con la password definita:

Per utilizzare il nuovo archivio dati protetto, è necessario innanzitutto aprirlo facendo clic sul pulsante ***Apri subito***. Una volta aperto, l'archivio dati protetto verrà visualizzato nel computer come un nuovo disco virtuale. Assegnare all'archivio una lettera dal menu a discesa (*è possibile selezionare solo i dischi attualmente liberi*). In genere, non è consentito scegliere le lettere C *(assegnata solitamente al disco rigido)*, A *(unità disco floppy)* o D *(unità DVD)*. Tenere presente che ogni volta che si sblocca un archivio dati protetto è possibile scegliere una lettera diversa per l'unità tra quelle disponibili.

Come sbloccare l'archivio dati protetto

Quando si tenta di accedere nuovamente all'archivio dati protetto viene richiesto di sbloccarlo utilizzando la password definita:

Digitare nel campo di testo la password di autorizzazione e fare clic sul pulsante ***Sblocca***. Se non si riesce a ricordare la password, fare clic su ***Suggerimento*** per visualizzare il suggerimento per la password definito al momento della creazione dell'archivio dati protetto. Il nuovo archivio dati protetto verrà visualizzato nella panoramica degli archivi dati protetti come SBLOCCATO e sarà possibile aggiungere o rimuovere i file al suo interno in base alle esigenze.

6.2. Protezione esplorazione Web

La ***Protezione esplorazione Web*** è composta da due servizi: ***LinkScanner Surf-Shield*** e ***Online Shield***.

- ***LinkScanner Surf-Shield*** protegge dal numero sempre crescente di minacce transitorie presenti sul Web. Queste minacce possono nascondersi in qualsiasi tipo di sito Web, da quelli degli enti governativi, a quelli di grandi marchi famosi, a quelli di piccole aziende, e raramente restano in questi siti per più di 24 ore. LinkScanner protegge gli utenti analizzando le pagine Web a cui puntano tutti i collegamenti presenti nella pagina Web visualizzata e garantendo che le pagine siano sicure nel momento cruciale, ovvero nell'attimo in cui si sta per fare clic sul collegamento. ***Il componente LinkScanner Surf-Shield non è destinato alla protezione delle piattaforme server.***

- ***Online Shield*** è un tipo di protezione permanente in tempo reale che esegue la scansione del contenuto delle pagine Web visitate (e dei possibili file in esse contenuti) persino prima che vengano visualizzate nel browser Web o scaricate nel computer. Online Shield rileva se la pagina che sta per essere aperta contiene javascript dannosi e ne impedisce la visualizzazione. Inoltre, riconosce il malware contenuto in una pagina arrestandone immediatamente il download per impedirne il trasferimento nel computer. Si tratta di un potente strumento di protezione che blocca il contenuto pericoloso delle pagine Web quando si tenta di aprirle, impedendone il download sul computer. Se questa funzionalità è abilitata, quando si fa clic sul collegamento o si digita l'URL di un sito pericoloso, l'apertura della pagina Web verrà bloccata immediatamente impedendo che il PC dell'utente venga infettato. È importante tenere presente che le pagine Web dannose possono infettare il computer con il semplice accesso al sito infetto. ***Il componente Online Shield non è destinato alle piattaforme server.***

Comandi della finestra di dialogo

Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del rispettivo pannello di servizio. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo è possibile trovare i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono *(LinkScanner Surf-Shield o Online Shield)*:

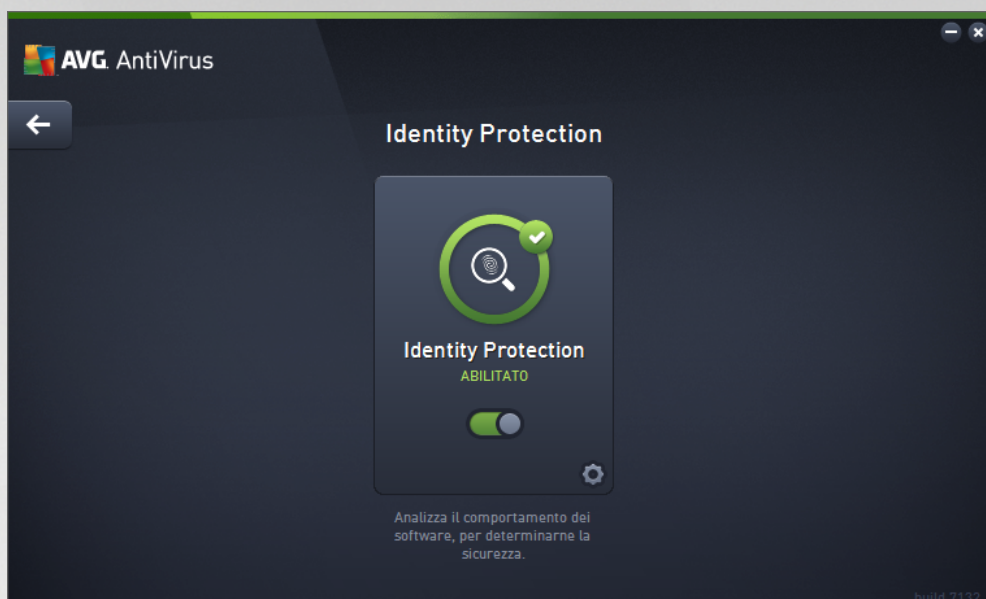
Attivato / Disattivato: questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa ***Attivato***, ovvero indica che il servizio di protezione LinkScanner Surf-Shield / Online Shield è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato***, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se per qualche ragione si desidera disattivare il servizio, per mettere in guardia dai possibili rischi verrà subito visualizzato il simbolo rosso di ***Avviso*** e l'utente verrà informato che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Più precisamente, verrà aperta la rispettiva finestra di dialogo e l'utente potrà configurare il servizio selezionato, ovvero LinkScanner Surf-Shield o Online Shield. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione tramite **AVG AntiVirus**, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti.

Freccia: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all'interfaccia utente principale con la panoramica dei componenti.

6.3. Identity Protection

Il componente ***Identity Protection*** esegue il servizio ***Identity Shield*** che assicura la protezione costante delle risorse digitali contro le nuove minacce online:

- ***Identity Protection*** è un servizio anti-malware che protegge da tutti i tipi di malware (*spyware, bot, furto di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus. Identity Protection è destinato alla prevenzione di attacchi da parte di malintenzionati volti a sottrarre password, dati dei conti bancari, numeri delle carte di credito e altri importanti dati digitali tramite qualsiasi tipo di software dannoso *(malware)* in grado di colpire il PC. L'applicazione assicura che tutti i programmi in esecuzione nel PC o nella rete condivisa funzionino correttamente. Identity Protection rileva e blocca i comportamenti sospetti e protegge il computer da tutti i nuovi malware. Identity Protection fornisce al computer la protezione in tempo reale da minacce nuove e sconosciute. Monitora tutti i processi *(compresi quelli nascosti)* e oltre 285 diversi schemi di comportamento ed è in grado di determinare se nel sistema si stanno verificando operazioni dannose. Per tale motivo, può rilevare minacce non ancora descritte nel database dei virus. Quando un codice sconosciuto entra nel computer viene immediatamente controllato, per verificarne l'eventuale comportamento dannoso, e tracciato. Se si determina che il file è dannoso, Identity Protection rimuove il codice spostandolo in Quarantena virus e annulla le modifiche apportate al sistema *(iniezioni di codice, modifiche del registro, apertura di porte e così via)*. Non è necessario avviare una scansione per essere protetti. La tecnologia è proattiva, richiede raramente l'aggiornamento ed è sempre attiva.

Comandi della finestra di dialogo

Nella finestra di dialogo sono disponibili i seguenti controlli:

- ***Attivato / Disattivato***: questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde rappresenta lo stato ***Attivato***, ovvero indica che il servizio di protezione Identity Protection è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato***, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se è necessario disattivare il servizio, per mettere in guardia dai possibili rischi viene visualizzato il segnale rosso di ***Avviso*** con la notifica che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

- ***Impostazioni***: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero Identity Protection. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione incluso in **AVG AntiVirus**, tuttavia si sconsiglia agli utenti meno esperti di apportare modifiche.

- ***Freccia***: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica dei componenti nell'interfaccia utente principale.

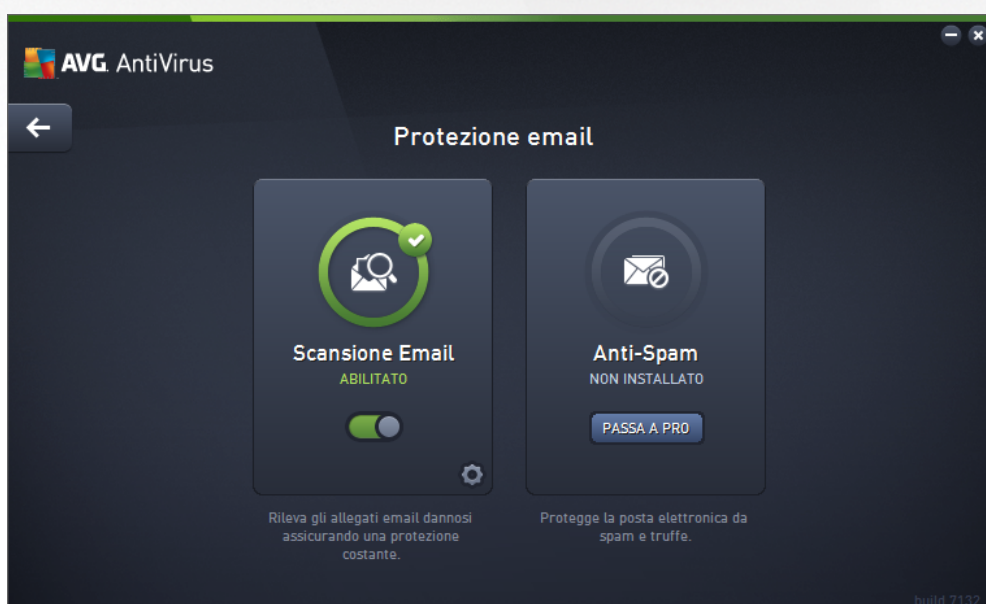
Purtroppo in **AVG AntiVirus** il servizio Identity Alert non è incluso. Se si desidera utilizzare questo tipo di protezione, fare clic sul pulsante ***Aggiorna per attivare*** per essere reindirizzati alla pagina Web dedicata in cui è possibile acquistare la licenza di Identity Alert.

Tenere presente che anche nelle edizioni AVG Premium Security, il servizio Identity Alert è attualmente disponibile solo nei seguenti paesi: Stati Uniti, Regno Unito, Canada e Irlanda.

6.4. Protezione email

Il componente ***Protezione email*** include i due seguenti servizi di protezione: ***Scansione Email*** e ***Anti-Spam*** *(il servizio Anti-Spam è accessibile solo nelle edizioni Internet/Premium Security)*.

- ***Scansione Email***: una delle origini più comuni di virus e trojan è la posta elettronica. Phishing e spam rendono la posta elettronica una grande fonte di rischio. Gli account email gratuiti sono quelli che presentano più probabilità di ricevere questo tipo di messaggi dannosi *(poiché raramente impiegano una tecnologia antispam)* e gli utenti domestici si affidano moltissimo a questo tipo di email. Inoltre, gli utenti domestici aumentano l'esposizione ad attacchi tramite email poiché navigano spesso in siti sconosciuti e compilano moduli online con dati personali *(ad esempio l'indirizzo email)*. Di solito le società utilizzano account aziendali, filtri antispam e altri accorgimenti per ridurre il rischio. Il componente Protezione email è responsabile della scansione di tutti i messaggi email inviati o ricevuti. Ogni volta che viene rilevato un virus in un'email, questo viene immediatamente spostato in Quarantena virus. Il componente, inoltre, può filtrare alcuni tipi di allegati email e aggiungere un testo di certificazione ai messaggi non infetti. ***Il componente Scansione Email non è destinato alle piattaforme server.***

- ***Anti-Spam*** consente di controllare tutti i messaggi email in arrivo e di contrassegnare quelli indesiderati come spam *(il termine "spam" indica messaggi di posta indesiderati, per lo più pubblicità di prodotti o servizi, inviate in massa e simultaneamente a un enorme numero di indirizzi di posta elettronica, che intasano le cassette postali dei destinatari. Lo spam non rientra nella categoria dei messaggi email commerciali legittimi per i quali i consumatori hanno fornito il consenso.)*. Anti-Spam può modificare l'oggetto dell'email *(identificata come spam)* aggiungendo una stringa di testo speciale. Sarà quindi possibile filtrare rapidamente i messaggi email nel client email. Il componente Anti-Spam utilizza diversi metodi di analisi per elaborare ciascun messaggio email, offrendo il massimo livello di protezione possibile contro i messaggi email indesiderati. Anti-Spam utilizza un database aggiornato regolarmente per il rilevamento dello spam. È inoltre possibile utilizzare i server RBL *(database pubblici di indirizzi email di spammer noti)* e aggiungere manualmente indirizzi email alla whitelist *(indirizzi da non contrassegnare mai come spam)* e alla blacklist *(indirizzi da contrassegnare sempre come spam)*.

Comandi della finestra di dialogo

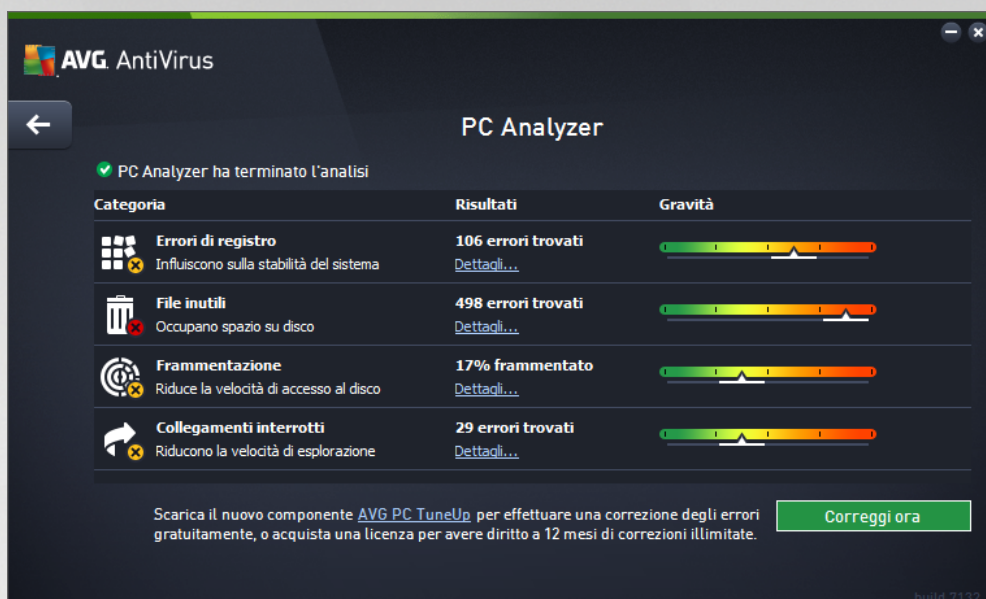
Per passare da una sezione all'altra della finestra di dialogo, è possibile fare clic in qualsiasi punto del rispettivo pannello di servizio. Il pannello viene evidenziato in una tonalità di blu più chiara. In entrambe le sezioni della finestra di dialogo è possibile trovare i seguenti controlli. La funzionalità è la stessa, indipendentemente dal servizio di protezione a cui appartengono *(Scansione Email o Anti-Spam)*:

Attivato / Disattivato: questo pulsante è simile a un semaforo, sia nell'aspetto che nella funzionalità. Fare clic per passare da una posizione all'altra. Il colore verde significa ***Attivato***, ovvero indica che il servizio di protezione è attivo e completamente funzionante. Il colore rosso rappresenta lo stato ***Disattivato***, ovvero indica che il servizio è disabilitato. A meno che non sussista un motivo valido per disattivare il servizio, si consiglia di mantenere le impostazioni predefinite per tutte le configurazioni di protezione. Le impostazioni predefinite assicurano prestazioni ottimali dell'applicazione e massima protezione. Se per qualche ragione si desidera disattivare il servizio, per mettere in guardia dai possibili rischi verrà subito visualizzato il simbolo rosso di ***Avviso*** e l'utente verrà informato che la protezione non è completa. ***Tenere presente che è necessario riattivare il servizio il prima possibile.***

Impostazioni: facendo clic su questo pulsante si viene reindirizzati all'area delle impostazioni avanzate. Verrà aperta la relativa finestra di dialogo e sarà possibile configurare il servizio selezionato, ovvero Scansione Email o Anti-Spam. Nell'area delle impostazioni avanzate è possibile modificare la configurazione di ogni servizio di protezione tramite **AVG AntiVirus**, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti.

Freccia: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all'interfaccia utente principale con la panoramica dei componenti.

6.5. PC Analyzer

Il componente ***PC Analyzer*** è uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni complessive del computer. Si apre attraverso l'opzione ***Ottimizza le prestazioni*** disponibile nella finestra di dialogo dell'interfaccia utente principale o tramite la stessa opzione disponibile nel menu di scelta rapida dell'icona di AVG nella barra delle applicazioni. Sarà quindi possibile visualizzare l'avanzamento dell'analisi e i relativi risultati direttamente nel grafico:

È possibile analizzare le seguenti categorie: errori di registro, file inutili, frammentazione e collegamenti interrotti:

- ***Errori di registro*** fornisce il numero di errori presenti nel Registro di Windows che potrebbero causare rallentamenti del computer o la visualizzazione di messaggi di errore.

- ***File inutili*** fornisce il numero di file che consumano spazio su disco e che molto probabilmente sono superflui. In genere si tratta di file temporanei di vario tipo e dei file presenti nel Cestino.

- ***Frammentazione*** consente di calcolare la percentuale di disco rigido frammentata, ovvero utilizzata per molto tempo per cui al momento numerosi file si trovano sparsi in diverse parti del disco fisico.

- ***Collegamenti interrotti*** individua collegamenti non più funzionanti, che conducono a posizioni inesistenti e così via.

La panoramica dei risultati presenta il numero di problemi del sistema rilevati, divisi in base alle relative categorie controllate. I risultati dell'analisi verranno inoltre visualizzati graficamente nella colonna ***Gravità***.

Pulsanti di controllo

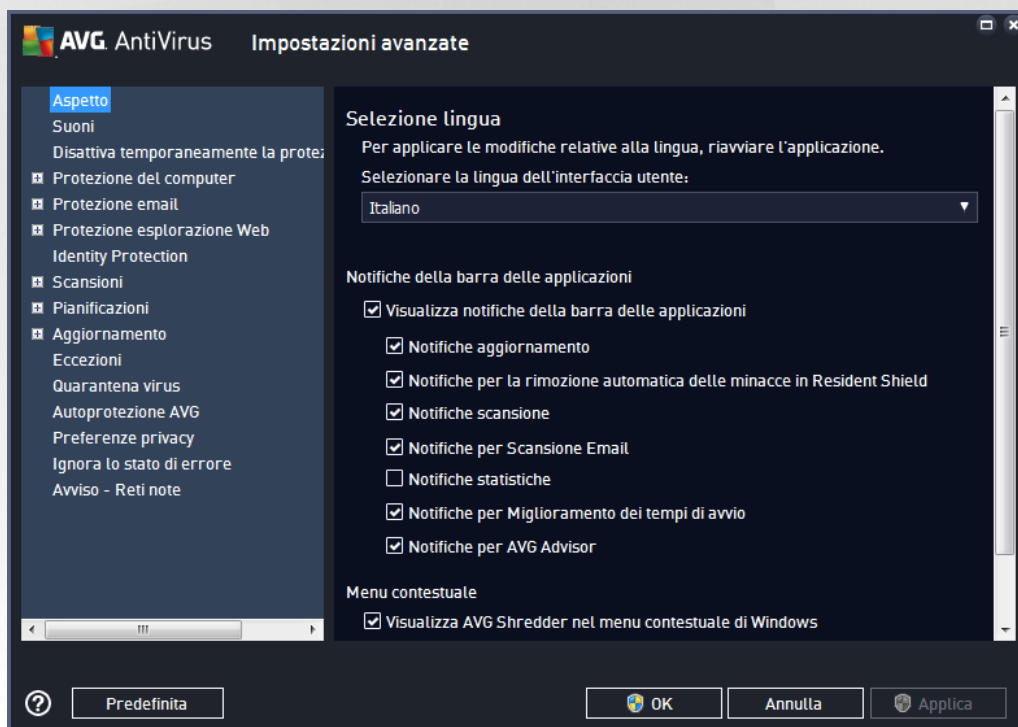
- ***Arresta analisi*** (*visualizzato durante l'esecuzione dell'analisi*) : selezionare questo pulsante per interrompere l'analisi del computer.

- ***Correggi ora*** *(visualizzato al termine dell'analisi*): la funzionalità di PC Analyzer in **AVG AntiVirus** è limitata all'analisi dello stato presente del PC. Tuttavia, AVG fornisce uno strumento avanzato per l'analisi e la correzione dettagliate del sistema che consente di migliorare la velocità e le prestazioni complessive del computer. Fare clic sul pulsante per essere reindirizzati alla pagina Web dedicata in cui sono disponibili ulteriori informazioni.

7. Impostazioni avanzate di AVG

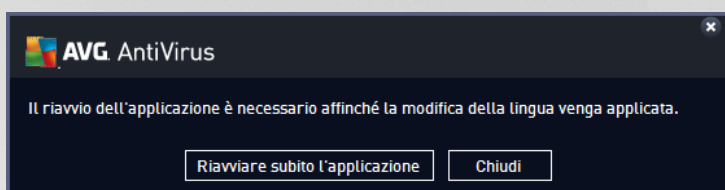
Le opzioni di configurazione avanzata di **AVG AntiVirus** sono disponibili in una nuova finestra denominata ***Impostazioni AVG avanzate***. La finestra è suddivisa in due sezioni: la parte sinistra fornisce una struttura di esplorazione per accedere alle opzioni di configurazione del programma. Selezionare il componente di cui si desidera modificare la configurazione (*o una parte specifica*) per aprire la finestra di dialogo di modifica nella sezione destra della finestra.

7.1. Aspetto

La prima voce della struttura di esplorazione, ***Aspetto***, fa riferimento alle impostazioni generali dell'interfaccia utente di **AVG AntiVirus** interfaccia utente e fornisce alcune opzioni di base relative al comportamento dell'applicazione:

Selezione lingua

Nella sezione ***Selezione lingua*** è possibile scegliere la lingua desiderata dal menu a discesa. La lingua selezionata verrà utilizzata per l'intera interfaccia utente di **AVG AntiVirus**. Nel menu a discesa sono presenti solo le lingue selezionate in precedenza per essere installate durante il processo di installazione e l'inglese (*sempre installato automaticamente per impostazione predefinita*). Per completare l'impostazione di **AVG AntiVirus** su un'altra lingua è necessario riavviare l'applicazione. Procedere come segue:

- Nel menu a discesa, selezionare la lingua desiderata per l'applicazione
- Confermare la selezione facendo clic sul pulsante ***Applica*** *nell'angolo inferiore destro della finestra di dialogo*
- Fare clic sul pulsante ***OK*** per confermare

- Viene visualizzata una nuova finestra di dialogo che comunica che per modificare la lingua dell'applicazione è necessario riawiare **AVG AntiVirus**
- Fare clic sul pulsante ***Riavvia subito AVG*** per confermare il riawio del programma e attendere alcuni istanti l'applicazione della modifica della lingua:

Notifiche della barra delle applicazioni

In questa sezione è possibile eliminare la visualizzazione delle notifiche della barra delle applicazioni sullo stato dell'applicazione **AVG AntiVirus**. Per impostazione predefinita, le notifiche della barra delle applicazioni vengono visualizzate. Si consiglia di mantenere questa impostazione. Le notifiche di sistema comunicano, ad esempio, l'awio del processo di scansione o aggiornamento o una modifica dello stato di un componente di **AVG AntiVirus** . Questi awisi devono essere tenuti nella dovuta considerazione.

Tuttavia, se non si desidera visualizzare tali notifiche o si desidera visualizzarne solo alcune *(correlate a un particolare componente di AVG AntiVirus)*, è possibile specificare le proprie preferenze selezionando/ deselezionando le seguenti opzioni:

- ***Visualizza notifiche della barra delle applicazioni*** *(attivata per impostazione predefinita)*: per impostazione predefinita, tutte le notifiche vengono visualizzate. Deselezionare questa voce per disattivare completamente la visualizzazione delle notifiche di sistema. Quando è attivata, è possibile selezionare inoltre le notifiche specifiche da visualizzare:
    - ***Notifiche aggiornamento*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative **AVG AntiVirus** all'awio, all'avanzamento e alla finalizzazione del processo di aggiornamento.
    - ***Notifiche per la rimozione automatica delle minacce in Resident Shield*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare o meno le informazioni relative ai processi di salvataggio, copia e apertura dei file (*questa configurazione viene visualizzata solo se l'opzione Correzione automatica di Resident Shield è attiva*).
    - ***Notifiche scansione*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative all'awio automatico, all'avanzamento e ai risultati della scansione pianificata.
    - ***Notifiche per Scansione Email*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative alla scansione di tutti i messaggi email in entrata e in uscita.
    - ***Notifiche statistiche*** *(attivata per impostazione predefinita)*: consente di decidere se visualizzare le notifiche relative alle revisioni statistiche regolari nella barra delle applicazioni.
    - ***Notifiche sul miglioramento dei tempi di avvio*** *(disattivata per impostazione predefinita)*: consente di decidere se visualizzare le informazioni relative all'accelerazione dei tempi di awio

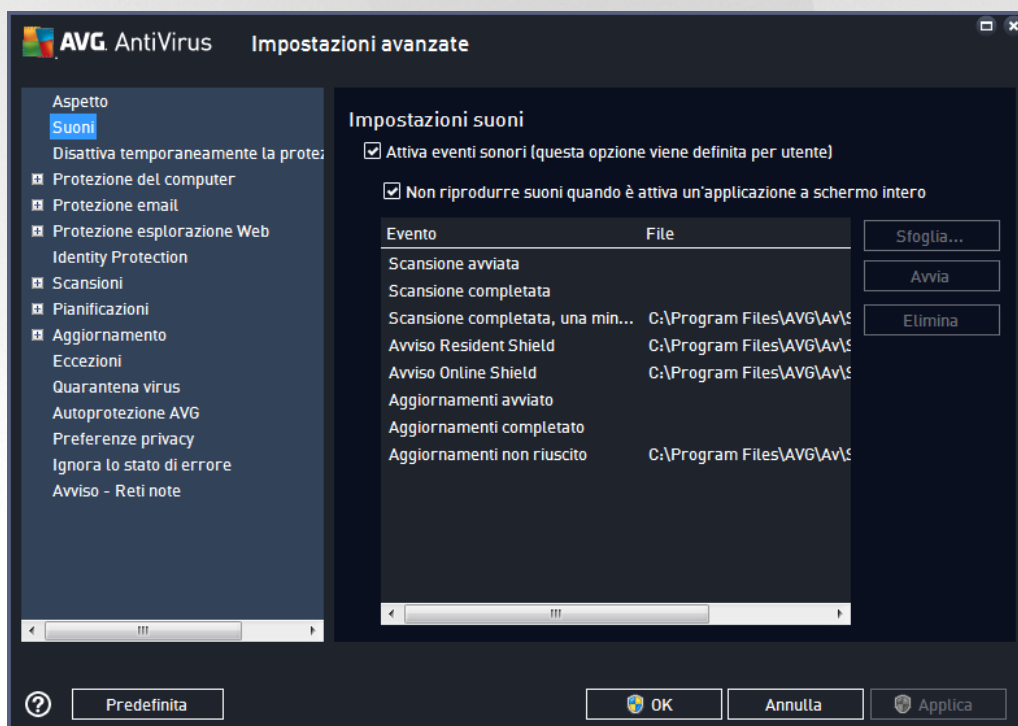
del computer.

- *Notifiche per AVG Advisor (attivata per impostazione predefinita):* consente di decidere se visualizzare le informazioni relative alle attività di AVG Advisor sotto forma di una finestra a comparsa sulla barra delle applicazioni.

Modalità gioco

Questa funzionalità è stata progettata per le applicazioni a schermo intero, per le quali eventuali notifiche a fumetto di AVG (*ad esempio quelle visualizzate all'avvio di una scansione pianificata*) potrebbero rappresentare una fonte di disturbo (*riducendole a icona o alterandone la grafica*). Per evitare questa situazione, mantenere selezionata l'opzione ***Abilita la Modalità gioco quando viene eseguita un'applicazione a schermo intero*** (*attivata per impostazione predefinita*).

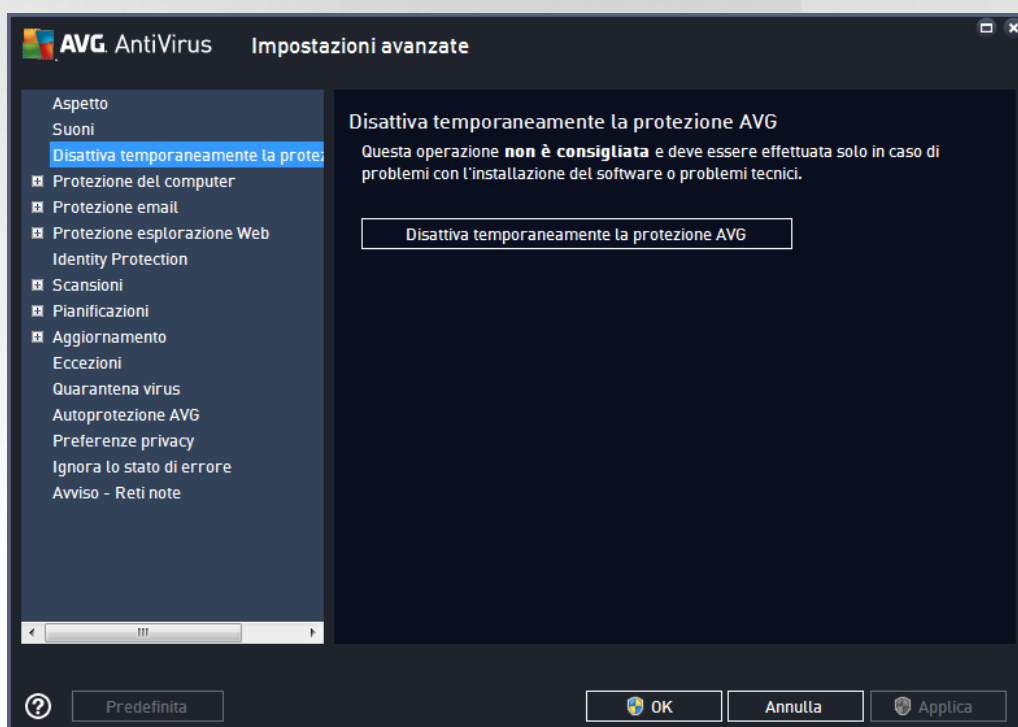
7.2. Suoni

Nella finestra di dialogo ***Impostazioni audio*** è possibile specificare se si desidera essere informati circa specifiche azioni di **AVG AntiVirus** tramite una notifica sonora:

Le impostazioni sono valide solo per l'account utente corrente, pertanto ogni utente del computer può disporre di impostazioni dei suoni personalizzate. Per consentire le notifiche sonore, mantenere l'opzione ***Attiva eventi sonori*** selezionata (*l'opzione è attivata per impostazione predefinita*) per attivare l'elenco di tutte le azioni correlate. Inoltre, è possibile selezionare l'opzione ***Non riprodurre suoni quando è attiva un'applicazione a schermo intero*** per eliminare le notifiche sonore quando potrebbero essere di disturbo *(vedere anche la sezione relativa alla modalità gioco del capitolo Impostazioni avanzate/Aspetto in questo documento).*

Pulsanti di controllo

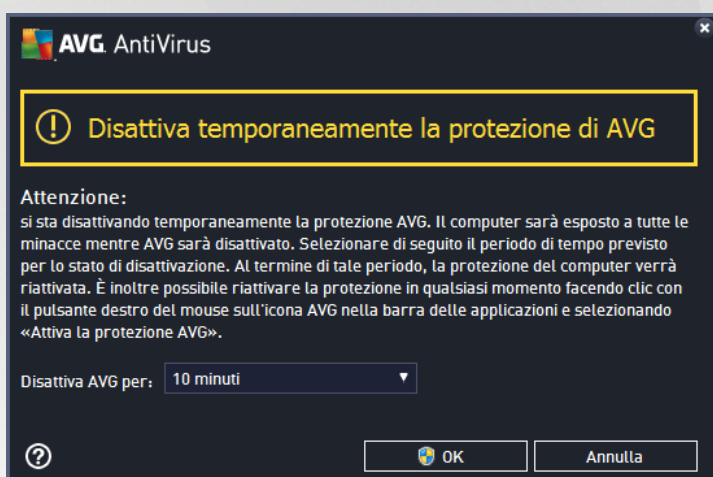
- ***Sfoglia...***: dopo aver selezionato l'evento dall'elenco, utilizzare il pulsante ***Sfoglia*** per ricercare nel disco il file audio desiderato da assegnare all'evento *(al momento sono supportati solo file *.wav).*
- ***Avvia***: per ascoltare il suono selezionato, evidenziare l'evento nell'elenco e fare clic sul pulsante ***Avvia***.
- ***Elimina***: utilizzare il pulsante ***Elimina*** per rimuovere il suono assegnato a uno specifico evento.

7.3. Disattivazione temporanea della protezione di AVG

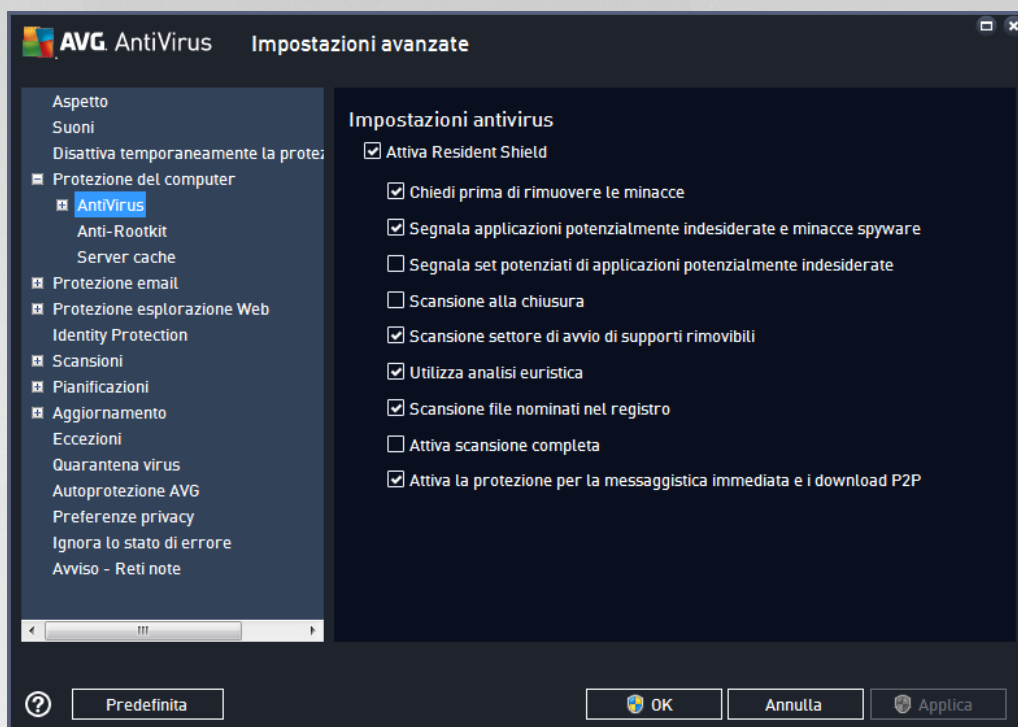
Nella finestra di dialogo ***Disabilitare temporaneamente la protezione di AVG*** è possibile disattivare l'intera protezione fornita da **AVG AntiVirus**.

Non utilizzare questa opzione se non è assolutamente necessario.

Nella maggior parte dei casi, ***non è necessario*** disattivare **AVG AntiVirus** prima di installare nuovi software o driver, neppure se il programma di installazione o la procedura guidata suggeriscono di chiudere tutti i programmi e le applicazioni in esecuzione per accertarsi che non si verifichino interruzioni indesiderate durante il processo di installazione. In caso di problemi durante l'installazione, provare innanzitutto a disattivare la protezione permanente *(nella finestra di dialogo collegata deselezionare la voce **Abilita Resident Shield**)*. Se fosse necessario disattivare temporaneamente **AVG AntiVirus**, lo si dovrà riattivare non appena possibile. Se si è connessi a Internet o a una rete mentre il software antivirus è disattivato, il computer sarà esposto a potenziali attacchi.

Come disattivare la protezione AVG

Selezionare la casella di controllo ***Disattiva temporaneamente la protezione di AVG*** e confermare la scelta facendo clic sul pulsante ***Applica***. Nella finestra di dialogo ***Disattiva temporaneamente la protezione di AVG*** aperta, specificare per quanto tempo si desidera disattivare **AVG AntiVirus**. Per impostazione predefinita, la protezione verrà disattivata per 10 minuti, tempo sufficiente per svolgere attività comuni quali l'installazione di un nuovo software e così via. È possibile impostare un periodo di tempo più lungo, tuttavia si consiglia di non utilizzare questa opzione se non è assolutamente necessario. Successivamente, tutti i componenti disattivati verranno riattivati automaticamente. È comunque possibile disattivare la protezione di AVG fino al successivo riavvio del computer. Nella finestra di dialogo ***Disattiva temporaneamente la protezione di AVG***

7.4. Protezione del computer

7.4.1. AntiVirus

AntiVirus e ***Resident Shield*** proteggono il computer in modo continuo da tutti i tipi noti di virus, spyware e malware in generale *(inclusi i cosiddetti malware dormienti e inattivi, ovvero i malware scaricati ma non ancora attivati)*.

Nella finestra di dialogo ***Impostazioni di Resident Shield*** è possibile attivare o disattivare completamente la protezione permanente selezionando/deselezionando la voce ***Attiva Resident Shield*** (*questa opzione è attivata per impostazione predefinita*). Inoltre, è possibile selezionare quali funzionalità della protezione permanente devono essere attivate:

- ***Chiedi prima di rimuovere le minacce*** (*attivata per impostazione predefinita*): selezionando questa opzione, Resident Shield non eseguirà alcuna azione automaticamente. Verrà invece visualizzata una finestra di dialogo che descrive la minaccia rilevata, consentendo di scegliere l'azione da eseguire. Se si mantiene deselezionata la casella, **AVG AntiVirus** tenterà automaticamente di correggere l'infezione e, nel caso sia impossibile, sposterà l'oggetto in Quarantena virus.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** (*disattivata per impostazione predefinita*): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione alla chiusura*** (*disattivata per impostazione predefinita*): la scansione alla chiusura assicura che AVG esegua la scansione di oggetti attivi (ad esempio applicazioni, documenti e così via) quando vengono aperti e anche quando vengono chiusi. Questa funzionalità consente di proteggere il computer da alcuni tipi di virus sofisticati.

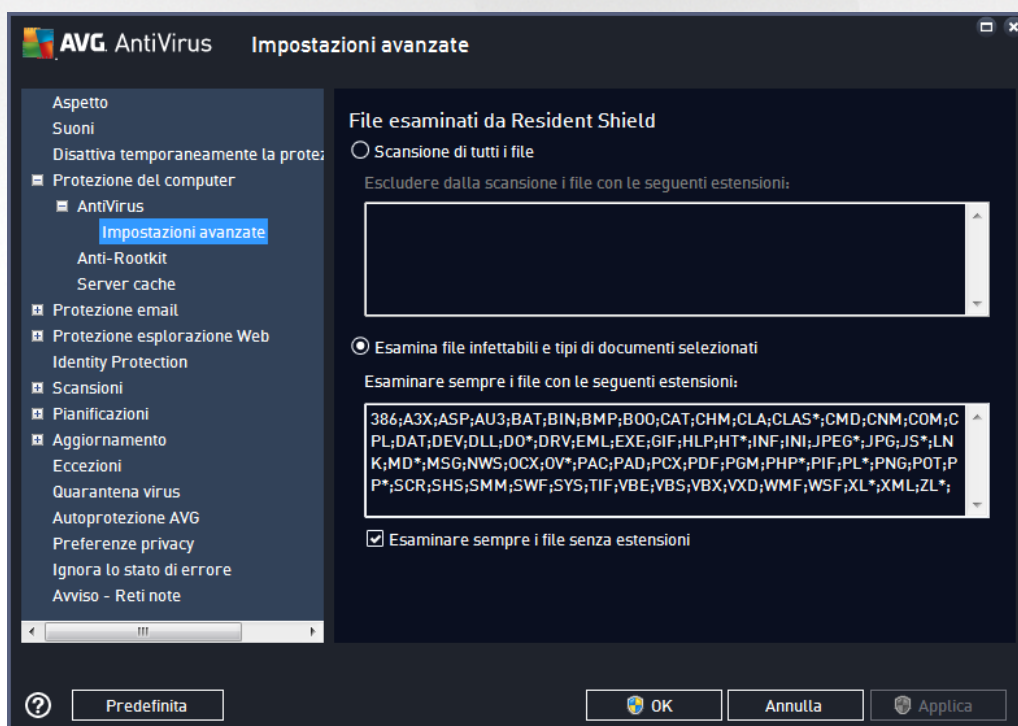
- ***Scansione settore di avvio di supporti rimovibili*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per eseguire la scansione dei settore di avvio dei dischi flash USB, dei dischi rigidi esterni e di altri supporti rimovibili per accertarsi che non contengano minacce.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica verrà utilizzata per il rilevamento (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Scansione file nominati nel registro*** (*attivata per impostazione predefinita*): questo parametro specifica che AVG sottoporrà a scansione tutti i file eseguibili aggiunti al registro di avvio per evitare che un'infezione nota venga eseguita al successivo avvio del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*) : in situazioni specifiche (*stati di estrema emergenza*) è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno accuratamente tutti gli oggetti potenzialmente minacciosi. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Attiva la protezione per la messaggistica immediata e i download P2P*** (*attivata per impostazione predefinita*) : selezionare questa voce se si desidera verificare che la comunicazione tramite messaggistica immediata (*ad esempio AIM, Yahoo!, ICQ, Skype, MSN Messenger e così via*) e i dati scaricati nelle reti peer-to-peer *(reti potenzialmente pericolose che consentono la connessione diretta tra client, senza un server, in genere sono utilizzate per condividere file musicali)* siano privi di virus.

Nella finestra di dialogo ***File esaminati da Resident Shield*** è possibile configurare i file che verranno sottoposti a scansione (*in base a estensioni specifiche*):

Selezionare la rispettiva casella di controllo per specificare se si desidera utilizzare l'opzione ***Scansione di***

tutti i file oppure solo ***Esamina file infettabili e tipi di documenti selezionati***. Per velocizzare la scansione e assicurare contemporaneamente il livello massimo di protezione, si consiglia di mantenere le impostazioni predefinite. In questo modo verranno sottoposti a scansione solo i file infettabili. Nella relativa sezione della finestra di dialogo è inoltre possibile trovare un elenco modificabile delle estensioni che definiscono i file inclusi nella scansione.

Selezionare l'opzione ***Esaminare sempre i file senza estensioni*** (*attivata per impostazione predefinita*) per assicurare che Resident Shield esegua anche la scansione dei file senza estensione e di formato sconosciuto. Si consiglia di mantenere questa funzionalità sempre attivata, in quanto i file senza estensione sono sospetti.

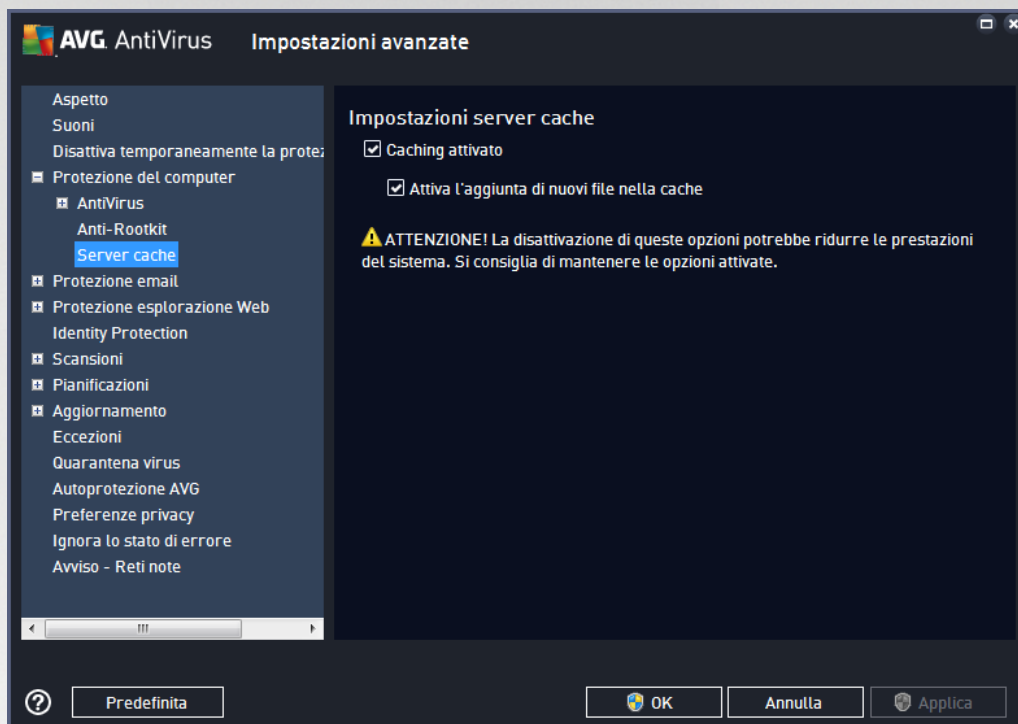
7.4.2. Anti-Rootkit

Nella finestra di dialogo ***Impostazioni di Anti-Rootkit*** è possibile modificare la configurazione del servizio ***Anti-Rootkit*** e i parametri specifici della scansione Anti-Rootkit. La scansione Anti-Rootkit è un processo predefinito incluso nella Scansione intero computer:

Scansione applicazioni e ***Scansione driver*** consentono di specificare in dettaglio gli elementi da includere nella scansione Anti-Rootkit. Queste impostazioni sono progettate per utenti esperti. Si consiglia di lasciare attivate tutte le opzioni. È inoltre possibile selezionare la modalità di scansione rootkit:

- ***Scansione rapida rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*)
- ***Scansione completa rootkit***: sottopone a scansione tutti i processi in esecuzione, i driver caricati e la cartella di sistema (*solitamente c:\Windows*), nonché tutte le unità locali (*inclusa l'unità di memoria flash, ma escluse le unità disco floppy/CD*)

7.4.3. Server cache

La finestra di dialogo ***Impostazioni del Server cache*** si riferisce al processo server cache destinato a velocizzare tutti i tipi di scansione di **AVG AntiVirus**:

Il server cache raccoglie e mantiene le informazioni relative ai file affidabili (*un file viene considerato affidabile se presenta la firma digitale di una fonte affidabile*). Questi file vengono quindi considerati sicuri e non necessitano di ulteriore scansione, pertanto vengono ignorati durante le scansioni.

La finestra di dialogo ***Impostazioni del Server cache*** offre le seguenti opzioni di configurazione:

- ***Caching attivato*** (*attivata per impostazione predefinita*) – deselezionare la casella per disattivare il ***Server cache*** e svuotare la memoria cache. Tenere presente che la scansione potrebbe subire un rallentamento e le prestazioni complessive del computer potrebbero ridursi, poiché per prima cosa ogni singolo file in uso verrà sottoposto alla scansione antivirus e antispyware.

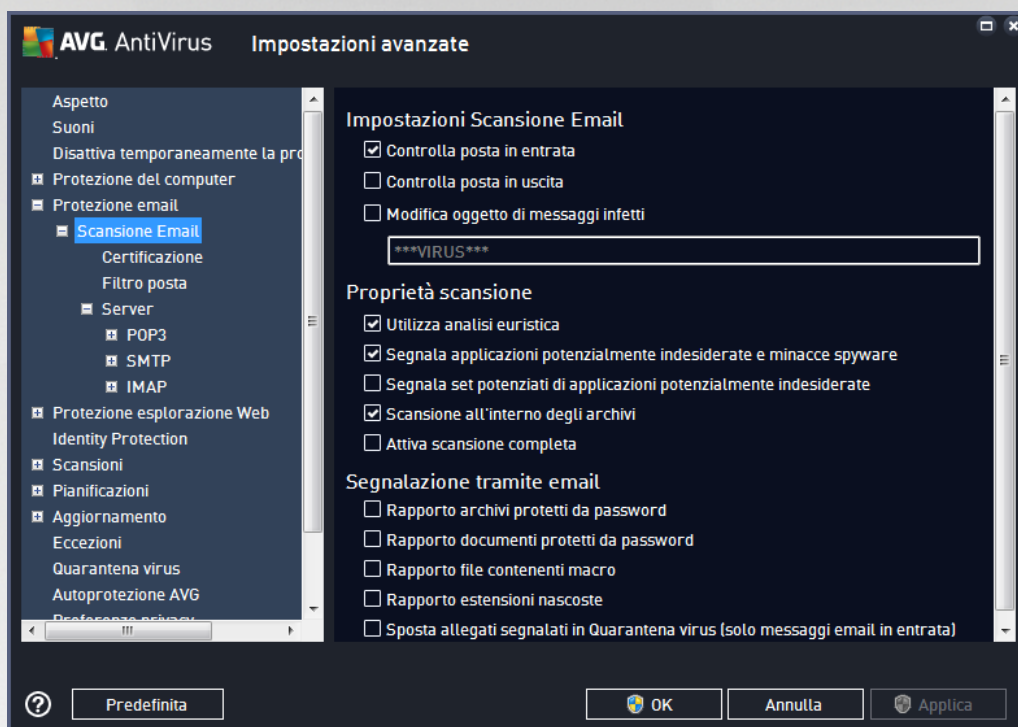
- ***Attiva l'aggiunta di nuovi file nella cache*** (*attivata per impostazione predefinita*) – deselezionare la casella per arrestare l'aggiunta di ulteriori file nella memoria cache. Tutti i file già presenti nella cache verranno mantenuti e utilizzati finché l'inserimento nella cache non verrà disattivato completamente o finché non verrà eseguito il successivo aggiornamento del database dei virus.

A meno che non sussista un motivo valido per disattivare il server cache, si consiglia di mantenere le impostazioni predefinite e lasciare attivate entrambe le opzioni. In caso contrario, la velocità e le prestazioni del sistema potrebbero ridursi notevolmente.

7.5. Scansione Email

In questa sezione è possibile modificare la configurazione dettagliata di Scansione Email e Anti-Spam:

7.5.1. Scansione Email

La finestra di dialogo ***Scansione Email*** è suddivisa in tre sezioni:

Scansione dell'email

In questa sezione è possibile configurare le seguenti impostazioni di base per i messaggi email in arrivo e/o in uscita:

- ***Controlla posta in entrata*** (*attivata per impostazione predefinita*): selezionare per attivare/disattivare l'opzione di scansione di tutti i messaggi email consegnati al client email
- ***Controlla posta in uscita*** (*disattivata per impostazione predefinita*): selezionare per attivare/ disattivare l'opzione di scansione di tutti i messaggi email inviati dall'account email
- ***Modifica oggetto di messaggi infetti*** (*disattivata per impostazione predefinita*): per essere informati del fatto che il messaggio email sottoposto a scansione si è rivelato infetto, selezionare questa voce e immettere il testo desiderato nel campo di testo. Il testo verrà aggiunto al campo "Oggetto" di ogni messaggio rilevato come infetto per facilitarne l'identificazione e il filtro. Il valore predefinito è ***VIRUS***. Si consiglia di mantenere questo valore.

Proprietà scansione

In questa sezione è possibile specificare la modalità di scansione dei messaggi email:

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): selezionare questa opzione per utilizzare il metodo di rilevamento tramite analisi euristica durante la scansione dei messaggi email. Se questa opzione è attivata, è possibile filtrare gli allegati dei messaggi email non solo per

estensione ma anche in base al contenuto effettivo dell'allegato. Il filtro può essere impostato nella finestra di dialogo Filtro posta.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione all'interno degli archivi*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per eseguire la scansione del contenuto degli archivi allegati ai messaggi email.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato da un virus o un attacco*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

Segnalazione allegati email

In questa sezione, è possibile impostare rapporti aggiuntivi sui file potenzialmente pericolosi o sospetti. Tenere presente che non verrà visualizzato alcun messaggio di avviso, verrà aggiunto soltanto un testo di certificazione alla fine del messaggio email e tutti i rapporti verranno elencati nella finestra di dialogo Rilevamento Protezione email:

- ***Segnala archivi protetti da password***: gli archivi (*ZIP, RAR e così via*) protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

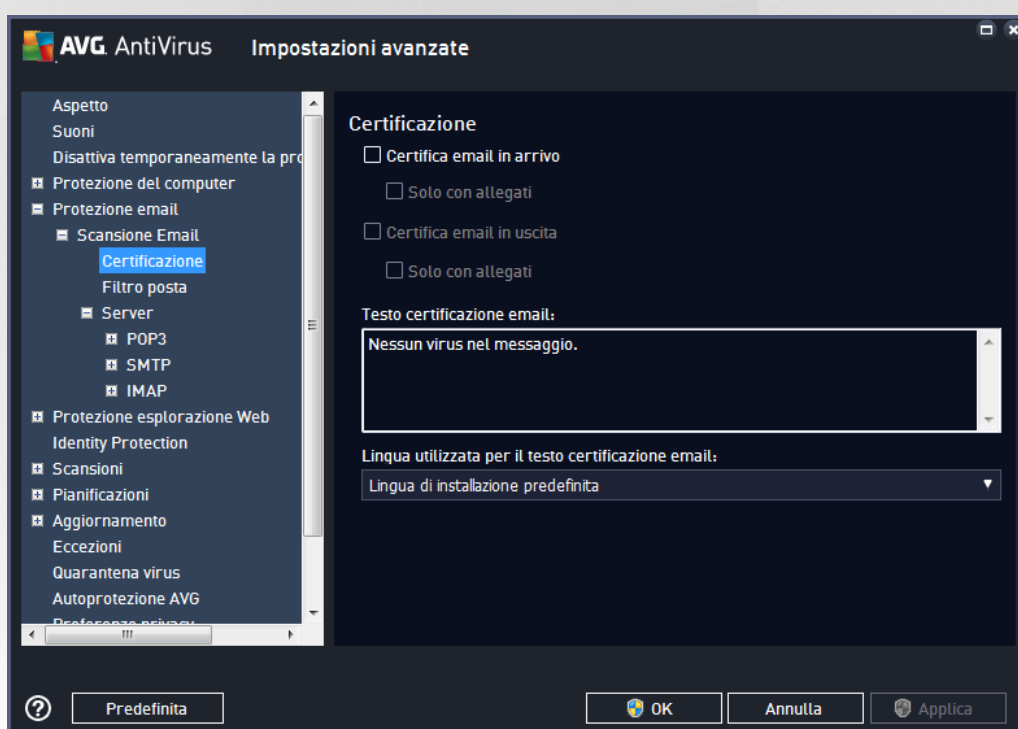
- ***Segnala documenti protetti da password***: i documenti protetti da password non possono essere sottoposti alla scansione antivirus. Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

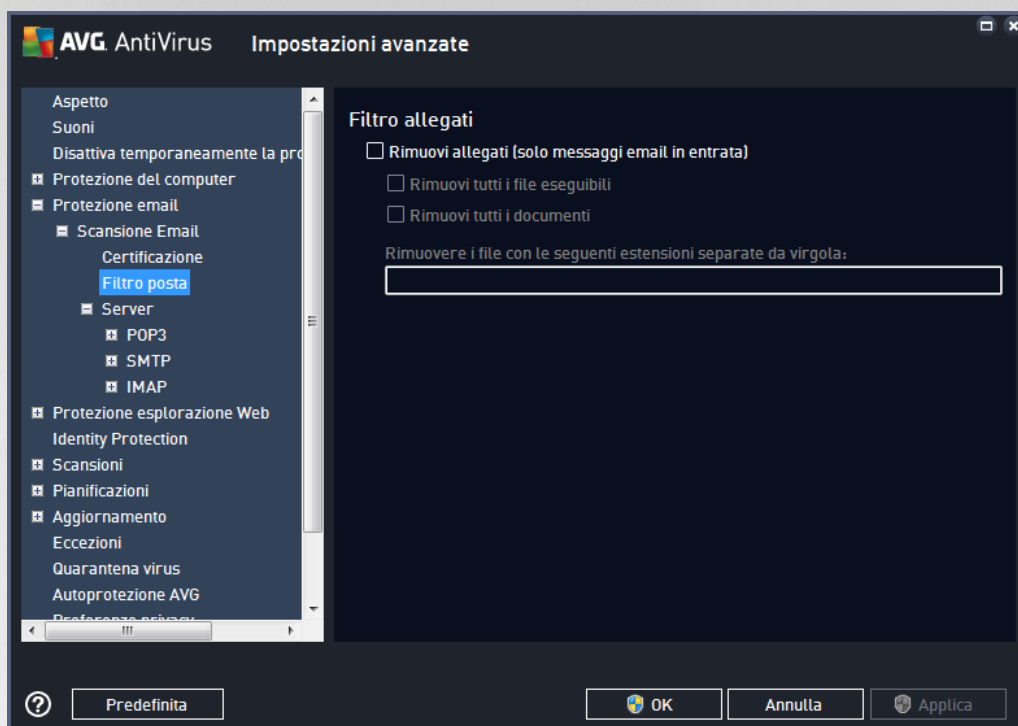
- ***Segnala file contenenti macro***: una macro è una sequenza di passaggi predefinita che consente di semplificare determinate attività (*le macro di MS Word, ad esempio, sono ampiamente conosciute*). Le macro possono contenere istruzioni potenzialmente pericolose. Selezionare la casella di controllo per assicurare che i file contenenti macro vengano segnalati come potenzialmente pericolosi.

- ***Segnala estensioni nascoste***: le estensioni nascoste possono far sembrare un file sospetto, ad esempio un file eseguibile del tipo "nomefile.txt.exe", come un innocuo file di testo del tipo "nomefile.txt". Selezionare la casella di controllo se si desidera che questi file vengano segnalati come potenzialmente pericolosi.

- ***Sposta allegati segnalati in Quarantena virus***: consente di specificare se si desidera ricevere una

notifica via email per gli archivi protetti da password, i documenti protetti da password, i file contenenti macro e/o i file con estensione nascosta rilevati come allegato del messaggio email sottoposto a scansione. Se viene identificato un messaggio simile durante la scansione, è possibile stabilire se l'oggetto infetto rilevato deve essere spostato in Quarantena virus.

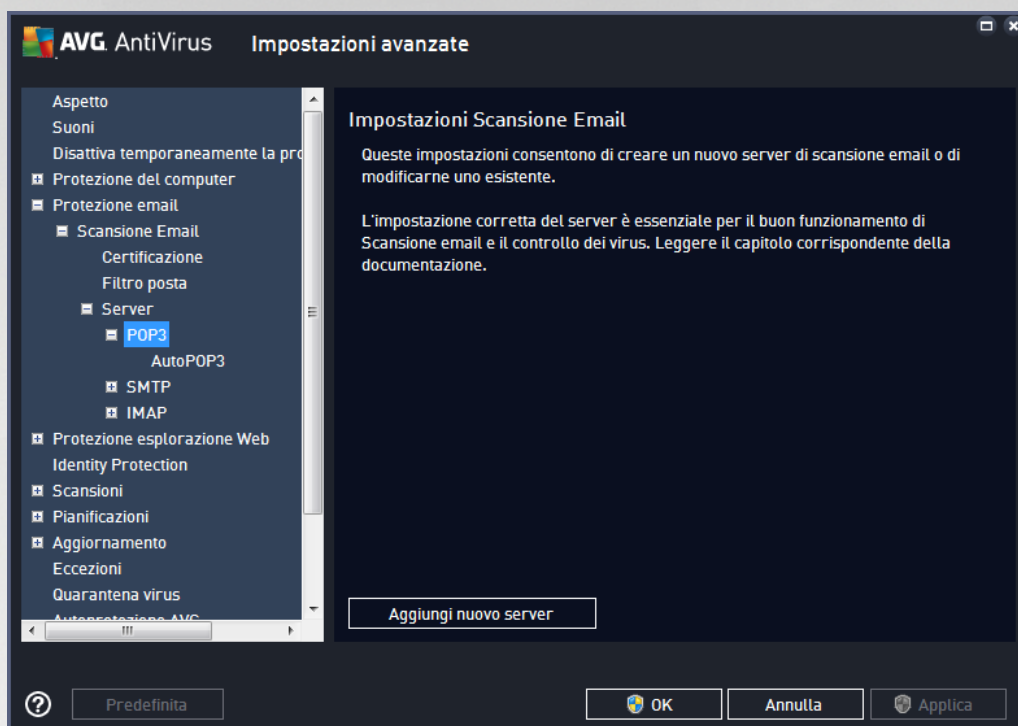
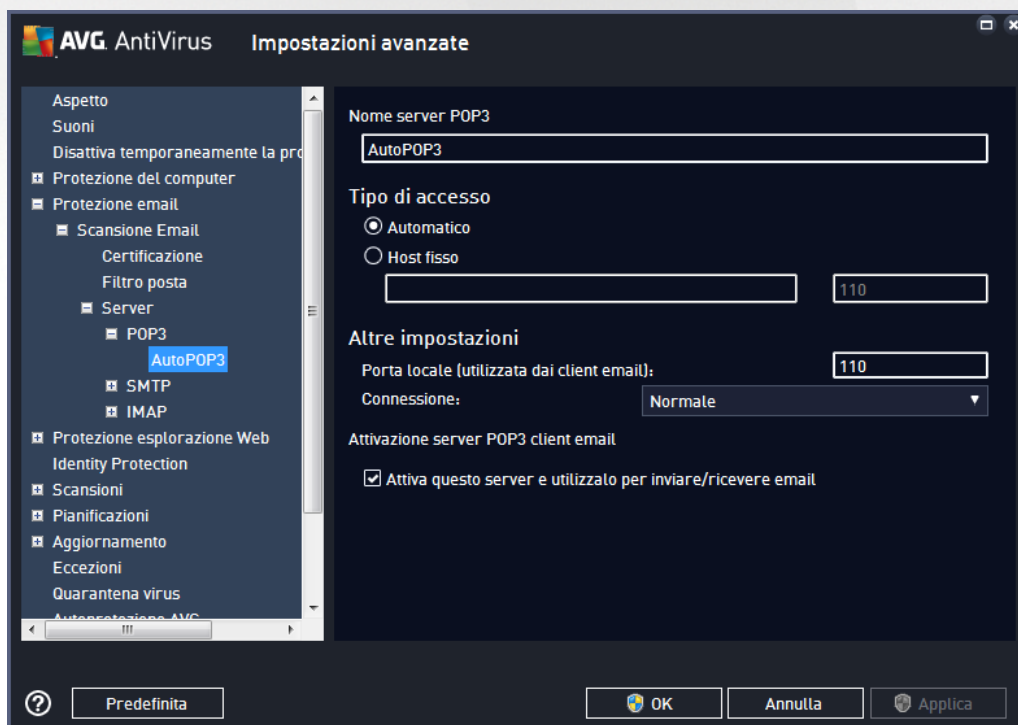
Nella finestra di dialogo ***Certificazione*** è possibile selezionare le caselle di controllo specifiche per specificare se si desidera certificare la posta in arrivo (***Certifica email in arrivo***) e/o la posta in uscita (***Certifica email in uscita***). Per ciascuna di queste opzioni è inoltre possibile specificare il parametro ***Solo con allegati*** per far sì che la certificazione venga aggiunta solo ai messaggi email con allegati:

Per impostazione predefinita, il testo di certificazione è composto da informazioni di base simili a *Nessun virus in questo messaggio.* Tuttavia, è possibile estendere o modificare queste informazioni in base alle esigenze, scrivendo il testo di certificazione desiderato nel campo ***Testo certificazione email***. Nella sezione ***Lingua utilizzata per il testo certificazione email*** è possibile inoltre definire in quale lingua verrà visualizzata la parte di certificazione generata automaticamente (*Nessun virus in questo messaggio*).

Nota: *tenere presente che solo il testo predefinito verrà visualizzato nella lingua richiesta e il testo personalizzato non verrà tradotto automaticamente.*

La finestra di dialogo ***Filtro allegati*** consente di impostare i parametri per la scansione degli allegati ai messaggi email. Per impostazione predefinita, l'opzione ***Rimuovi allegati*** è disattivata. Se si decide di attivarla, tutti gli allegati ai messaggi email rilevati come infetti o potenzialmente pericolosi verranno rimossi automaticamente. Se si desidera definire tipi specifici di allegati che devono essere rimossi, selezionare l'opzione corrispondente:

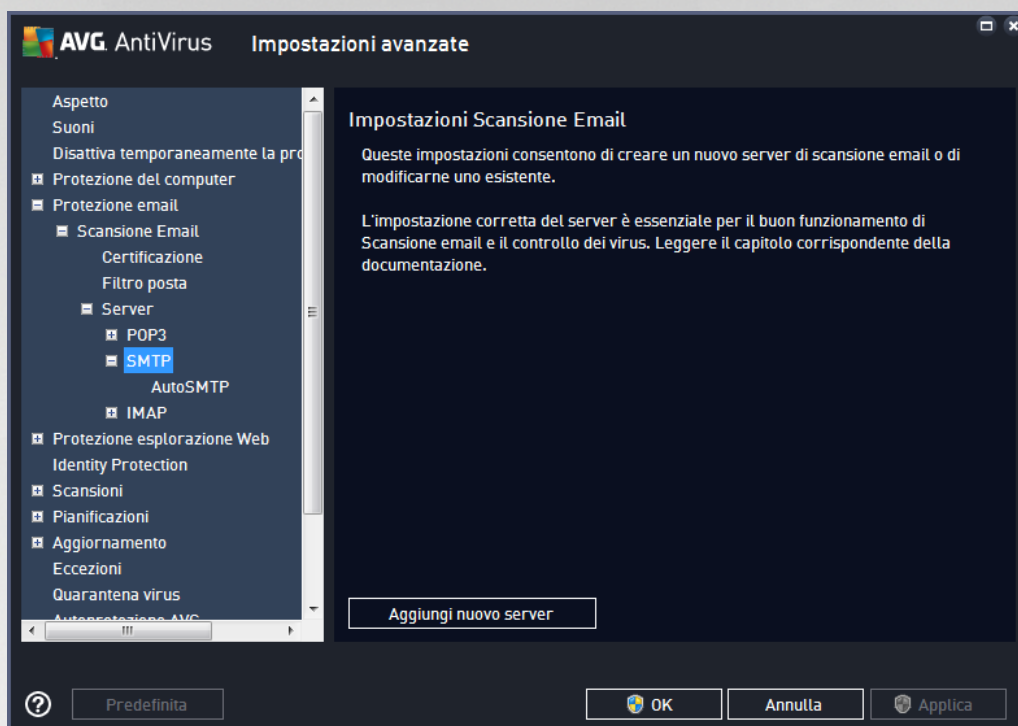
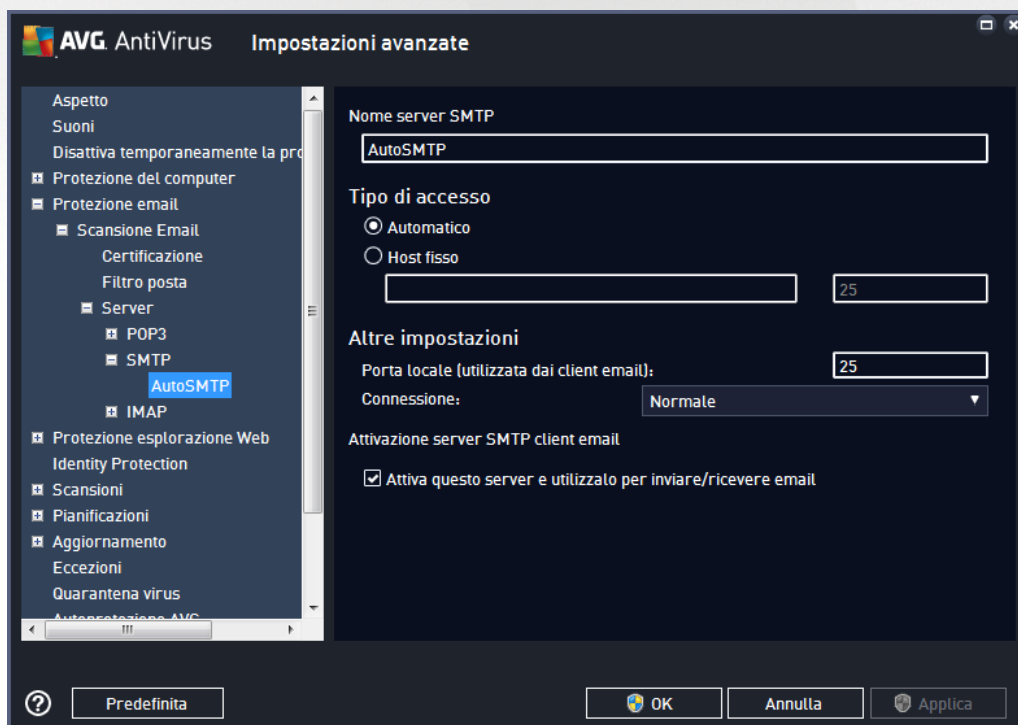
- ***Rimuovi tutti i file eseguibili***: tutti i file *.exe verranno eliminati
- ***Rimuovi tutti i documenti***: tutti i file *.doc, *.docx, *.xls e *.xlsx verranno eliminati
- ***Rimuovere i file con le seguenti estensioni separate da virgola***: verranno rimossi tutti i file con le estensioni specificate

Nella sezione ***Server*** è possibile modificare i parametri dei server di Scansione Email:

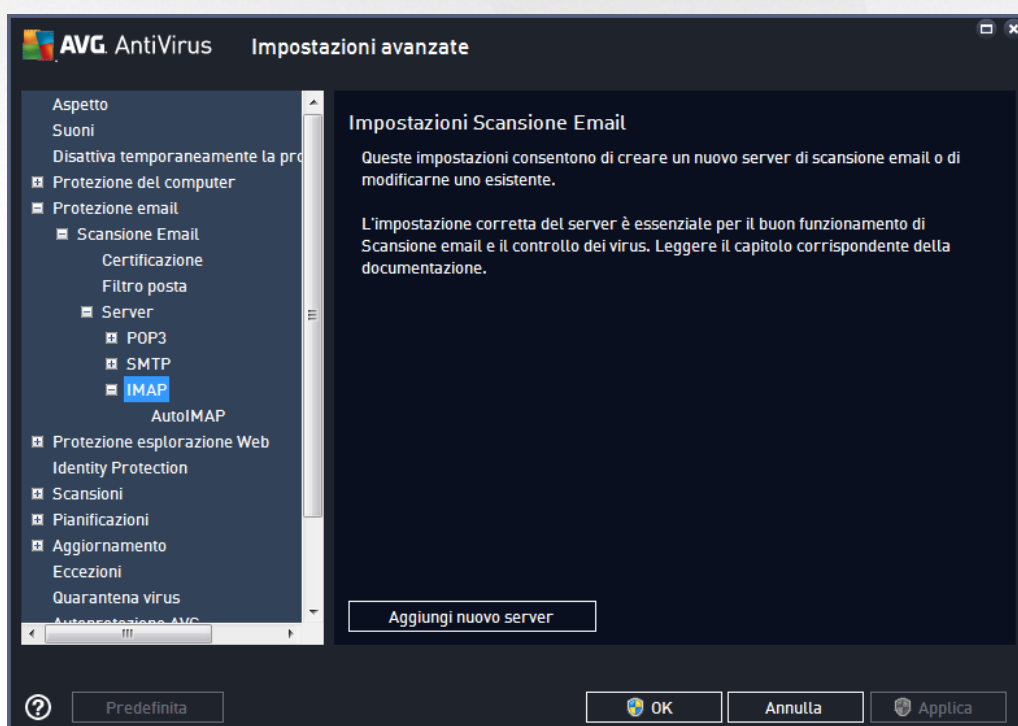
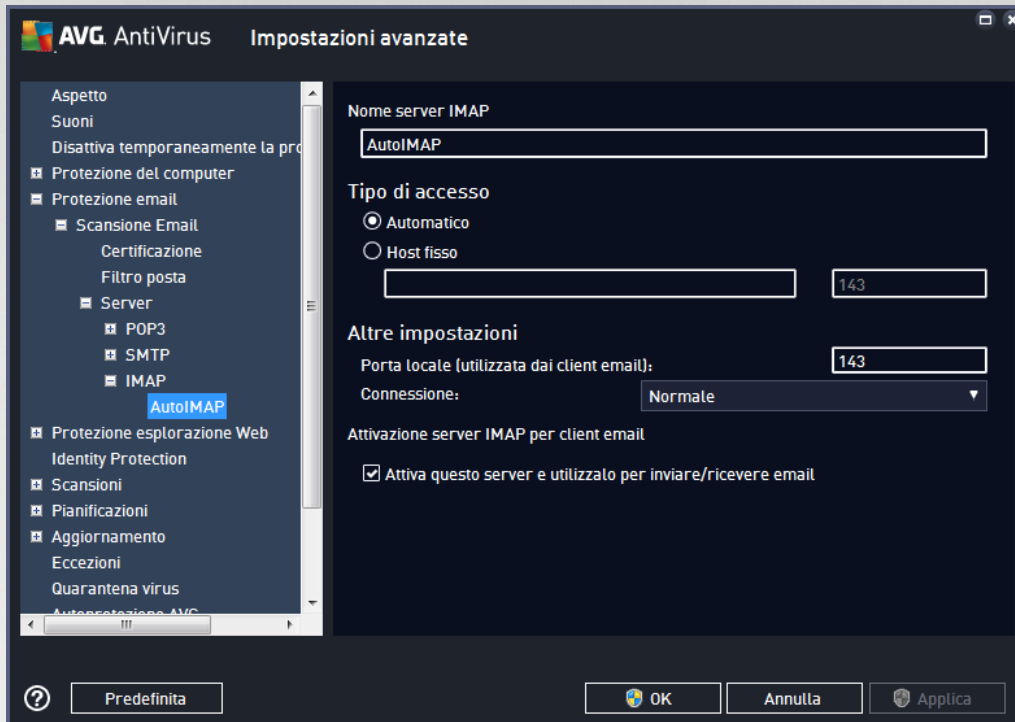
- Server POP3
- Server SMTP
- Server IMAP

Inoltre, è possibile definire nuovi server per la posta in arrivo o in uscita, utilizzando il pulsante ***Aggiungi nuovo server***.

Questa finestra di dialogo consente di impostare un nuovo server Scansione Email che utilizza il protocollo POP3 per la posta in entrata:

- ***Nome server POP3***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per*

aggiungere un server POP3, fare clic con il pulsante destro del mouse sulla voce POP3 nel menu di esplorazione a sinistra).

- ***Tipo di accesso***: definisce il metodo per determinare il server email utilizzato per la posta in arrivo:
    - o ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client email.
    - o ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server email. Il nome di accesso non verrà modificato. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio pop.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server email utilizza una porta non standard, è possibile specificare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, (*ad esempio pop.acme.com:8200*). La porta standard per la comunicazione POP3 è la numero 110.
- ***Altre impostazioni***: specifica parametri più dettagliati:
    - o ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione email. Nell'applicazione email sarà quindi necessario specificare tale porta come porta per la comunicazione POP3.
    - o ***Connessione***: nel menu a discesa è possibile specificare il tipo di connessione da utilizzare (*regolare/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità inoltre è disponibile solo se supportata dal server email di destinazione.
- ***Attivazione server POP3 client email***: selezionare/deselezionare questa voce per attivare o disattivare il server POP3 specificato

Questa finestra di dialogo consente di impostare un nuovo server Scansione Email che utilizza il protocollo SMTP per la posta in uscita:

- ***Nome server SMTP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per*

aggiungere un server SMTP, fare clic con il pulsante destro del mouse sulla voce SMTP nel menu di esplorazione a sinistra). Per i server "AutoSMTP" creati automaticamente questo campo è disattivato.

- ***Tipo di accesso***: definisce il metodo per determinare il server email utilizzato per la posta in uscita:
  - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client email
  - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server email. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server email utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio smtp.acme.com:8200*. La porta standard per la comunicazione SMTP è la numero 25.
- ***Altre impostazioni***: specifica parametri più dettagliati:
  - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione email. Nell'applicazione email sarà quindi necessario specificare tale porta come porta per la comunicazione SMTP.
  - ***Connessione***: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terzi. Questa funzionalità è disponibile solo se supportata dal server email di destinazione.
- ***Attivazione server SMTP per client email***: selezionare/deselezionare questa casella per attivare/disattivare il server SMTP specificato sopra

Questa finestra di dialogo consente di impostare un nuovo server Scansione Email che utilizza il protocollo IMAP per la posta in uscita:

- ***Nome server IMAP***: in questo campo è possibile specificare il nome dei nuovi server aggiunti (*per aggiungere un server IMAP, fare clic con il pulsante destro del mouse sulla voce IMAP nel menu di esplorazione a sinistra*).

- ***Tipo di accesso***: definisce il metodo per determinare il server email utilizzato per la posta in uscita:

  - ***Automatico***: l'accesso verrà effettuato automaticamente, in base alle impostazioni del client email

  - ***Host fisso***: in questo caso verrà sempre utilizzato il server specificato in questo campo. Specificare l'indirizzo o il nome del server email. Per il nome, è possibile utilizzare un nome di dominio (*ad esempio imap.acme.com*) o un indirizzo IP (*ad esempio 123.45.67.89*). Se il server email utilizza una porta non standard, è possibile digitare il nome della porta dopo quello del server utilizzando come separatore il segno di due punti, *ad esempio imap.acme.com:8200*. La porta standard per la comunicazione IMAP è la numero 143.

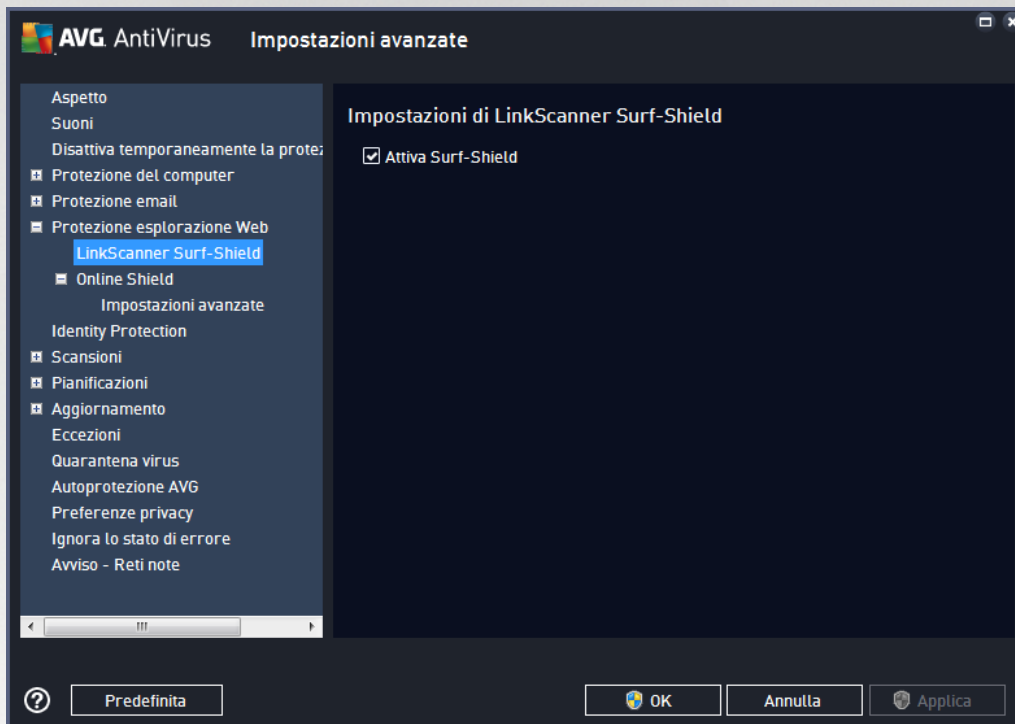
- ***Altre impostazioni***: specifica parametri più dettagliati:

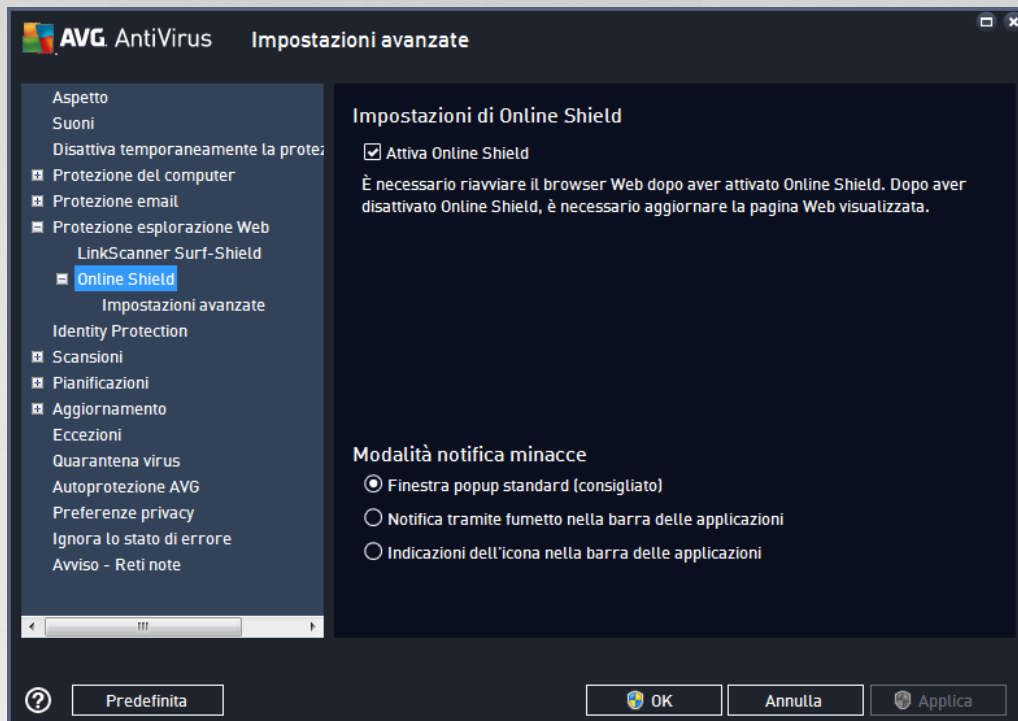
  - ***Porta locale***: specifica la porta su cui è prevista la comunicazione dall'applicazione email. Nell'applicazione email sarà quindi necessario specificare tale porta come porta per la comunicazione IMAP.

  - ***Connessione***: questo menu a discesa consente di specificare il tipo di connessione da utilizzare (*normale/SSL/SSL predefinito*). Se si sceglie la connessione SSL, i dati inviati verranno crittografati senza il rischio di essere rilevati o monitorati da terze parti. Questa funzionalità è disponibile solo se supportata dal server email di destinazione.

- ***Attivazione server IMAP per client email***: selezionare/deselezionare questa casella per attivare/disattivare il server IMAP specificato sopra

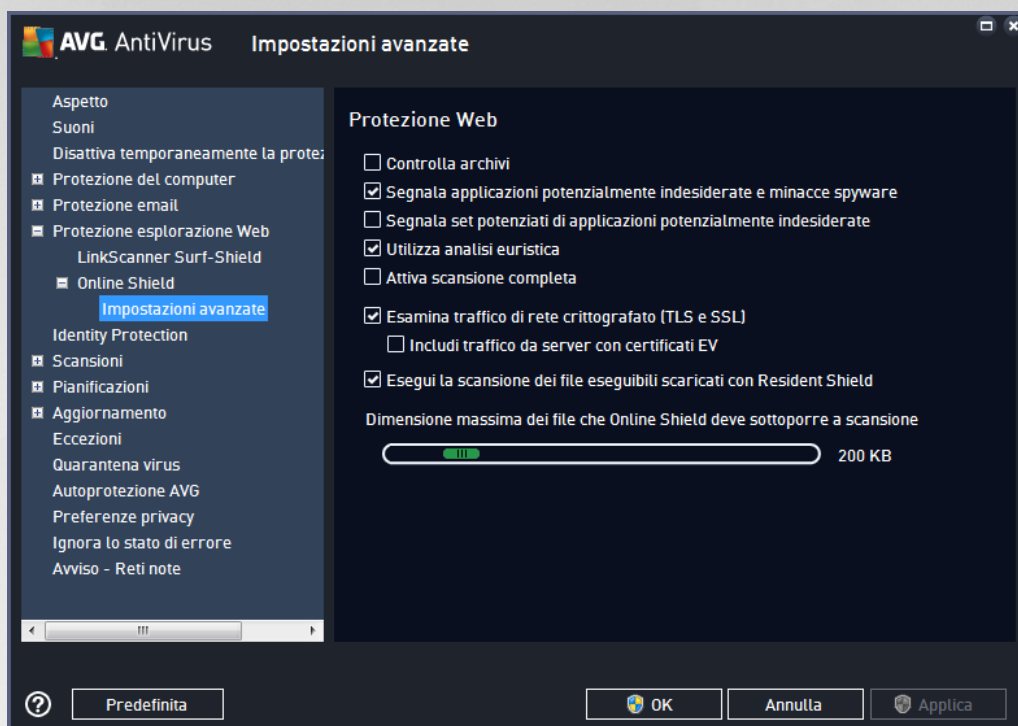
7.6. Protezione esplorazione Web

La finestra di dialogo ***Impostazioni LinkScanner*** consente di attivare/disattivare le seguenti funzioni:

- ***Abilita Surf-Shield***: (*attivata per impostazione predefinita*): protezione attiva, *in tempo reale,* da siti dannosi al momento dell'accesso. Le connessioni a siti dannosi noti e il relativo contenuto vengono bloccati non appena l'utente esegue l'accesso mediante un browser Web (*o qualsiasi altra applicazione che utilizza HTTP*).

7.6.1. Online Shield

La finestra di dialogo ***Online Shield*** presenta le seguenti opzioni:

- ***Abilita Online Shield*** *(attivata per impostazione predefinita)*: attiva/disattiva l'intero servizio ***Online Shield***. Per informazioni su altre impostazioni avanzate di ***Online Shield***, passare alla successiva finestra di dialogo denominata Protezione Web.

Modalità notifica minacce

Nella parte inferiore della finestra di dialogo, scegliere in che modo si desidera essere informati circa eventuali minacce rilevate: mediante una normale finestra a comparsa oppure mediante una notifica a fumetto o un'icona nell'area di notifica sulla barra delle applicazioni.

La finestra di dialogo ***Protezione Web*** consente di modificare la configurazione del componente relativamente alla scansione del contenuto di siti Web. L'interfaccia di modifica consente di configurare le seguenti opzioni di base:

- ***Controlla archivi*** (*disattivata per impostazione predefinita*): consente di eseguire la scansione del contenuto di eventuali archivi inclusi nella pagina Web da visualizzare.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** (*disattivata per impostazione predefinita*): selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): consente di eseguire la scansione del contenuto della pagina da visualizzare utilizzando il metodo dell'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*).

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita*): in situazioni specifiche (*se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile

selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

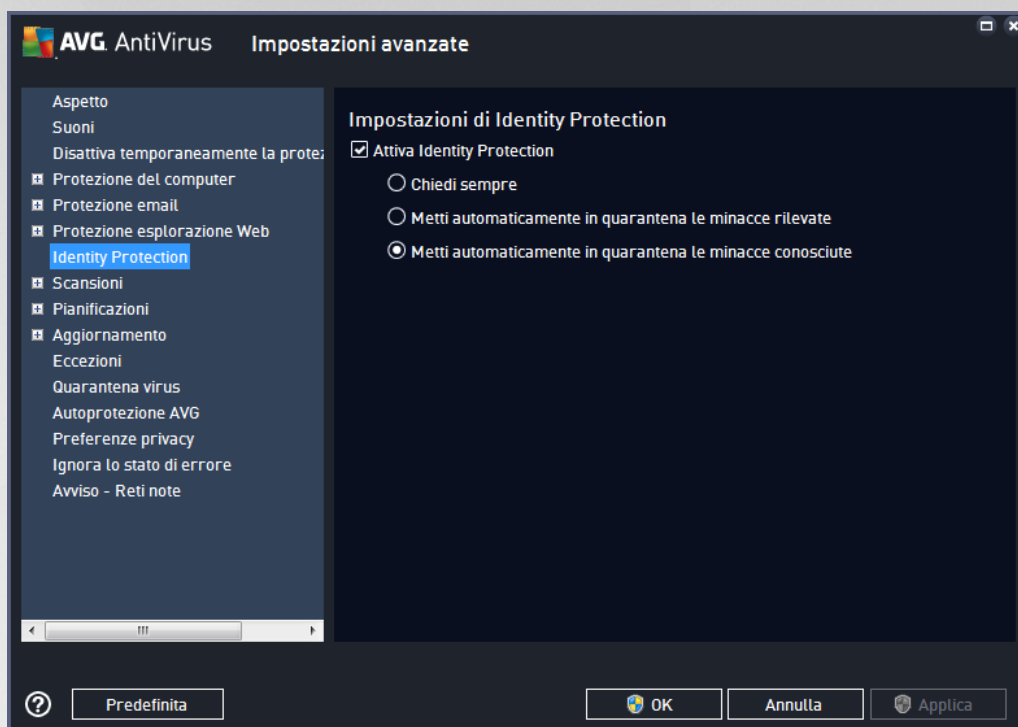
- ***Esamina traffico di rete crittografato (TLS e SSL)*** (*attivata per impostazione predefinita*): lasciare l'opzione selezionata per consentire ad AVG di analizzare anche le comunicazioni di rete crittografate, ovvero le connessioni tramite protocolli di sicurezza (SSL e la relativa versione più recente, TLS). Questa opzione si applica ai siti Web che utilizzano HTTPS e alle connessioni client email tramite TLS/SSL. Il traffico protetto viene decrittografato, esaminato per individuare eventuali malware e crittografato nuovamente per essere recapitato in modo sicuro al computer. In questa opzione è possibile selezionare anche ***Includi traffico da server con certificati EV***, per analizzare anche le comunicazioni di rete crittografate da server certificati con certificati di convalida estesa. L'emissione di un certificato EV richiede una convalida estesa da parte dell'autorità di certificazione, pertanto i siti Web che presentano tale certificato sono più affidabili *(ovvero hanno minori probabilità di distribuire malware)*. Per questo motivo, è possibile decidere di non sottoporre a scansione il traffico proveniente dai server certificati EV e ottenere quindi comunicazioni crittografate più rapide.

- ***Esegui scansione dei file eseguibili scaricati con Resident Shield*** (*attivata per impostazione predefinita*): consente di eseguire la scansione dei file eseguibili *(in genere con estensioni exe, bat, com)* dopo il download. Resident Shield esegue la scansione dei file prima del download per assicurare che non venga introdotto nessun file dannoso nel computer. Tuttavia, questa scansione è limitata dalla ***dimensione massima del file da sottoporre a scansione*** (vedere l'elemento successivo nella finestra di dialogo). I file di dimensioni maggiori, pertanto, vengono sottoposti a scansione una parte per volta e ciò si applica anche alla maggior parte dei file eseguibili. I file eseguibili possono eseguire diverse attività nel computer, perciò è fondamentale che siano completamente sicuri. Quindi, per una maggiore sicurezza, oltre alla scansione delle singole parti prima del download è opportuno sottoporre a scansione il file anche dopo il download. È consigliabile mantenere quest'opzione selezionata. Se questa opzione non viene attivata, si ha comunque la certezza che AVG rileverà qualsiasi codice potenzialmente pericoloso. Tuttavia, in genere non è in grado di valutare un file eseguibile nel complesso, perciò potrebbe creare dei falsi positivi.

Il dispositivo di scorrimento disponibile nella parte inferiore della finestra di dialogo consente di impostare la ***dimensione massima del file da esaminare***: se i file inclusi sono presenti nella pagina visualizzata è inoltre possibile eseguire la scansione del relativo contenuto prima che vengano scaricati nel computer. Tuttavia, la scansione di file di grandi dimensioni richiede parecchio tempo rallentando notevolmente il download della pagina Web. È possibile utilizzare il dispositivo di scorrimento per specificare la dimensione massima dei file che ***Online Shield*** deve ancora sottoporre a scansione. Anche se le dimensioni del file scaricato sono superiori a quelle specificate, e di conseguenza il file non verrà sottoposto a scansione da Online Shield, il computer è comunque protetto: se il file fosse infetto, verrebbe rilevato immediatamente da ***Resident Shield***.

7.7. Identity Protection

Identity Protection è un componente anti-malware che protegge il computer da qualsiasi tipo di malware (*spyware, bot, furti di identità e così via*) utilizzando tecnologie basate sul comportamento e fornisce la protezione zero day per i nuovi virus *(per una descrizione dettagliata delle funzionalità del componente, vedere il capitolo Dati personali*).

La finestra di dialogo ***Impostazioni di Identity Protection*** consente di attivare/disattivare le funzioni di base del componente Identity Protection:

Attiva Identity Protection (*attivata per impostazione predefinita*): deselezionare questa casella di controllo per disattivare il componente Dati personali. ***Si consiglia di non disattivare questo componente a meno che non sia assolutamente necessario.*** Quando Identity Protection è attivato, è possibile specificare l'azione da intraprendere quando viene rilevata una minaccia:

- ***Chiedi sempre***: quando viene rilevata una minaccia, verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione effettivamente da eseguire venga rimossa.

- ***Metti automaticamente in quarantena le minacce rilevate***: selezionare questa casella di controllo per spostare immediatamente tutte le potenziali minacce rilevate nell'area sicura di Quarantena virus. Se si mantengono le impostazioni predefinite, quando una minaccia viene rilevata verrà richiesto se spostarla in quarantena per assicurare che nessuna applicazione da eseguire venga rimossa.

- ***Metti automaticamente in quarantena le minacce conosciute*** (*attivata per impostazione predefinita*): mantenere selezionata questa opzione se si desidera che tutte le applicazioni rilevate come possibili malware vengano messe subito in Quarantena virus automaticamente.

7.8. Scansioni

La sezione delle impostazioni di scansione avanzate è suddivisa in quattro categorie che fanno riferimento a specifici tipi di scansione definiti dal fornitore del software:

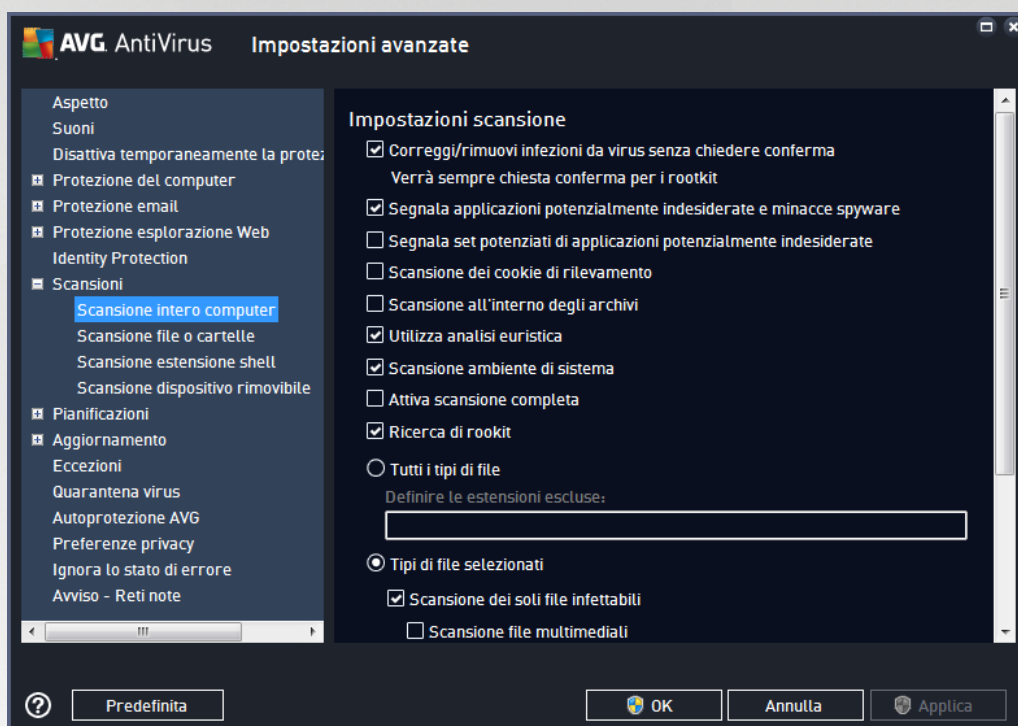
- Scansione intero computer: scansione predefinita standard dell'intero computer

- Scansione file o cartelle: scansione predefinita standard di aree selezionate del computer

- Scansione estensione shell: scansione specifica di un oggetto selezionato direttamente dall'ambiente Esplora risorse

- Scansione dispositivo rimovibile: scansione specifica di dispositivi rimovibili collegati al computer

7.8.1. Scansione intero computer

L'opzione ***Scansione intero computer*** consente di modificare i parametri di una delle scansioni predefinite dal fornitore del software, ossia Scansione intero computer:

Impostazioni scansione

Nella sezione ***Impostazioni scansione*** è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati a seconda delle necessità:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** (*attivata per impostazione predefinita*): se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** (*attivata per impostazione predefinita*): selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** (*disattivata per impostazione predefinita*): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del

computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro specifica che i cookie devono essere rilevati; (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici*).

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica della istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita)*: in situazioni specifiche (*se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** (*attivata per impostazione predefinita*): la scansione Anti-Rootkit cerca nel PC possibili rootkit, ovvero programmi e tecnologie che possono coprire l'attività dei malware nel computer. Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Inoltre, è necessario decidere quali elementi sottoporre a scansione

- ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione (*dopo il salvataggio, le virgole vengono sostituite da punto e virgola*).

- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile effettuare la ***Scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non si abbiano motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

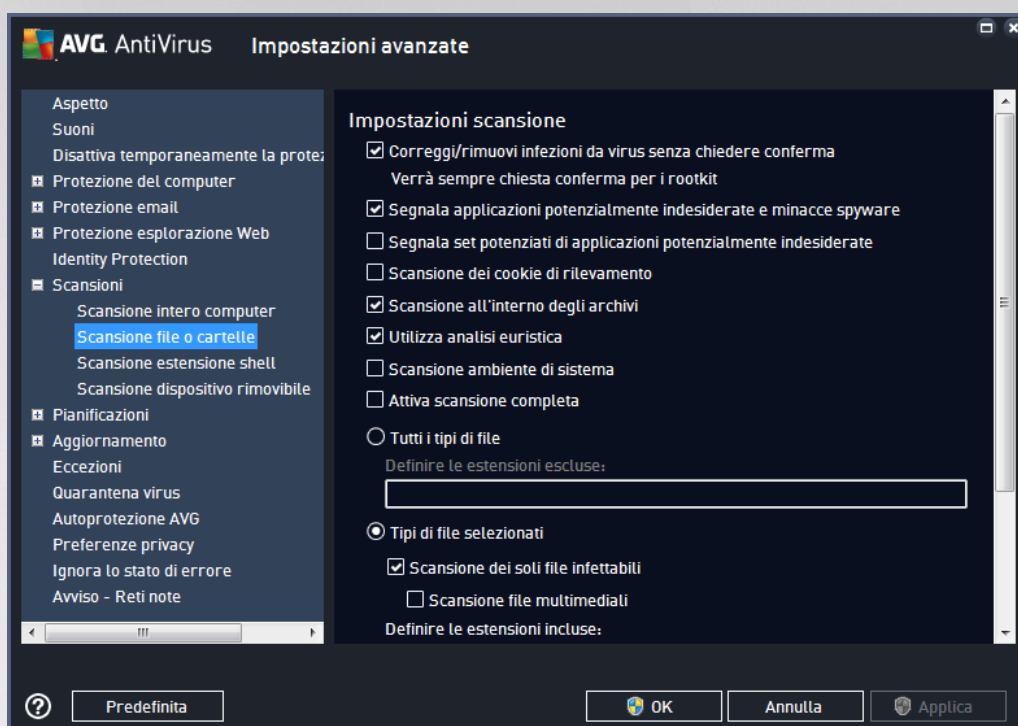
Regola la velocità di completamento della scansione

All'interno della sezione ***Regola la velocità di completamento della scansione*** è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non in uso*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

Imposta rapporti di scansione aggiuntivi...

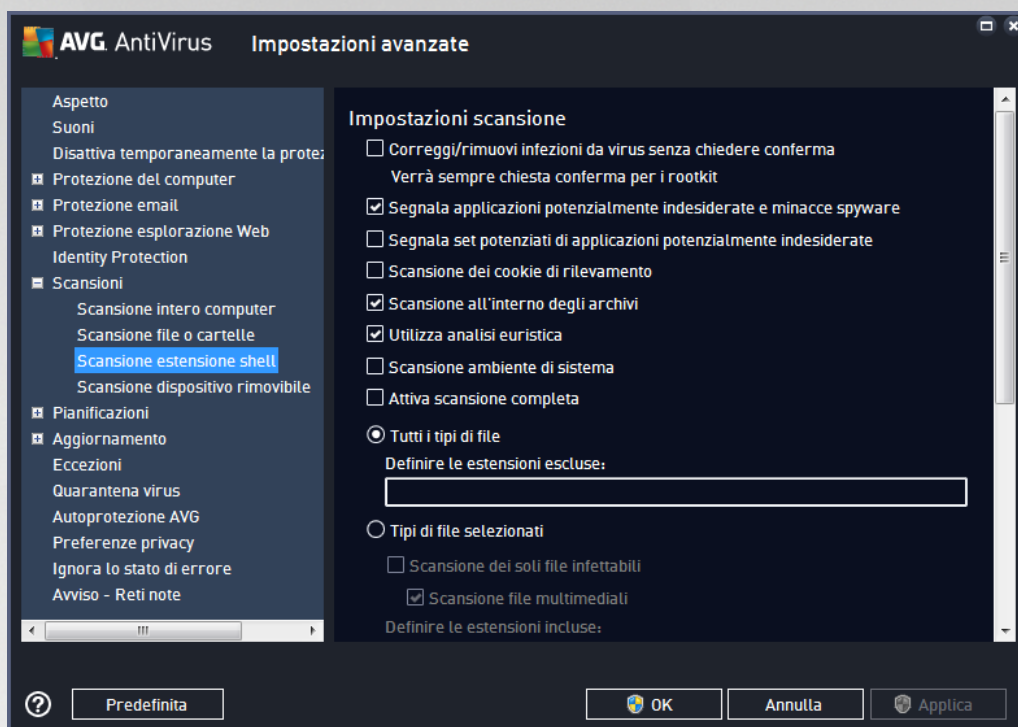
Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

7.8.2. Scansione file o cartelle

L'interfaccia di modifica di ***Scansione file o cartelle*** è quasi identica alla finestra di dialogo di modifica di Scansione intero computer, tuttavia le impostazioni predefinite sono più restrittive per Scansione intero computer:

Tutti i parametri impostati in questa finestra di dialogo di configurazione si applicano solo alle aree selezionate per la scansione con Scansione file o cartelle.

Nota: *per una descrizione dei parametri specifici, vedere il capitolo Impostazioni avanzate di AVG / Scansione / Scansione intero computer.*

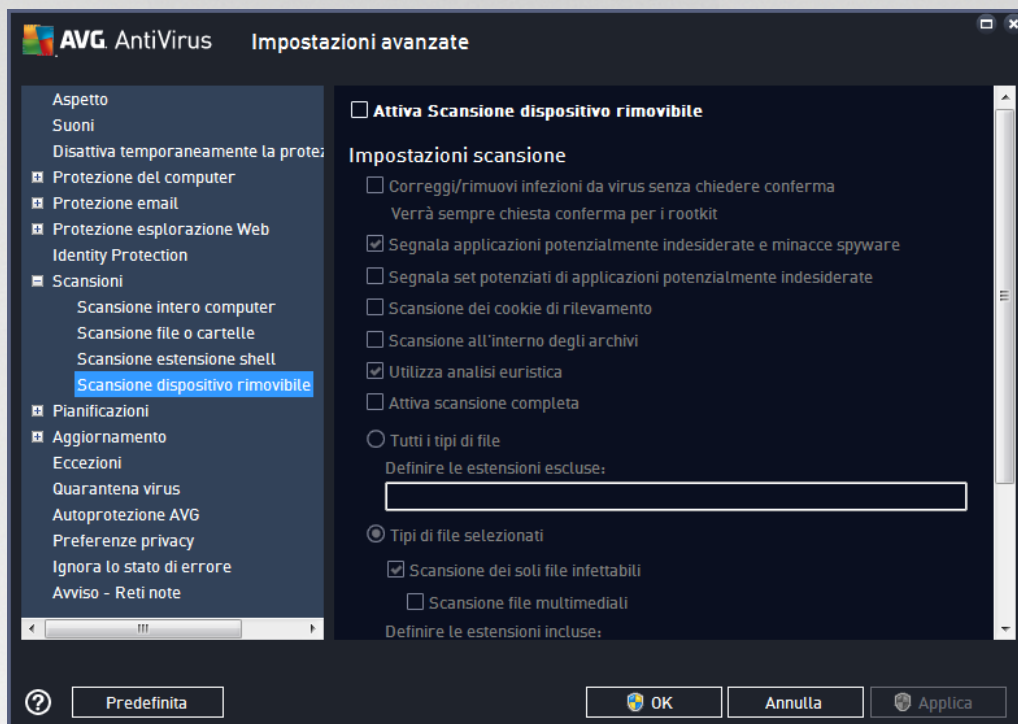
7.8.3. Scansione estensione shell

Analogamente a Scansione intero computer, ***Scansione estensione shell*** offre diverse opzioni per modificare la scansione predefinita dal fornitore del software. In questo caso, la configurazione è correlata alla scansione di oggetti specifici avviata direttamente dall'ambiente Esplora risorse (*estensione shell*), vedere il capitolo Scansione in Esplora risorse:

Le opzioni di modifica sono quasi identiche a quelle disponibili per Scansione intero computer, tuttavia, le impostazioni predefinite sono diverse (*ad esempio, per impostazione predefinita, Scansione intero computer non controlla gli archivi ma esegue la scansione dell'ambiente di sistema e viceversa per Scansione estensione shell*).

Nota: *per una descrizione dei parametri specifici, vedere il capitolo Impostazioni avanzate di AVG / Scansione / Scansione intero computer.*

Rispetto alla finestra di dialogo Scansione intero computer, la finestra di dialogo ***Scansione estensione shell*** include anche la sezione denominata ***Visualizzazione dei risultati e dell'avanzamento della scansione***, in cui è possibile specificare se si desidera accedere all'avanzamento della scansione e ai risultati della scansione dall'interfaccia utente di AVG. Inoltre, è possibile definire se il risultato della scansione deve essere visualizzato solo nel caso in cui venga rilevata un'infezione durante la scansione.

7.8.4. Scansione dispositivo rimovibile

Anche l'interfaccia di modifica di ***Scansione dispositivo rimovibile*** è molto simile alla finestra di dialogo di modifica di Scansione intero computer:

La ***Scansione dispositivo rimovibile*** viene avviata automaticamente quando si collega un dispositivo rimovibile al computer. Per impostazione predefinita, questa scansione è disattivata. Tuttavia, è molto importante effettuare la scansione dei dispositivi rimovibili per verificare la presenza di potenziali minacce poiché tali dispositivi rappresentano una delle fonti di infezione principali. Per avviare automaticamente questo tipo di scansione quando necessario, selezionare l'opzione ***Abilita scansione dispositivo rimovibile***.

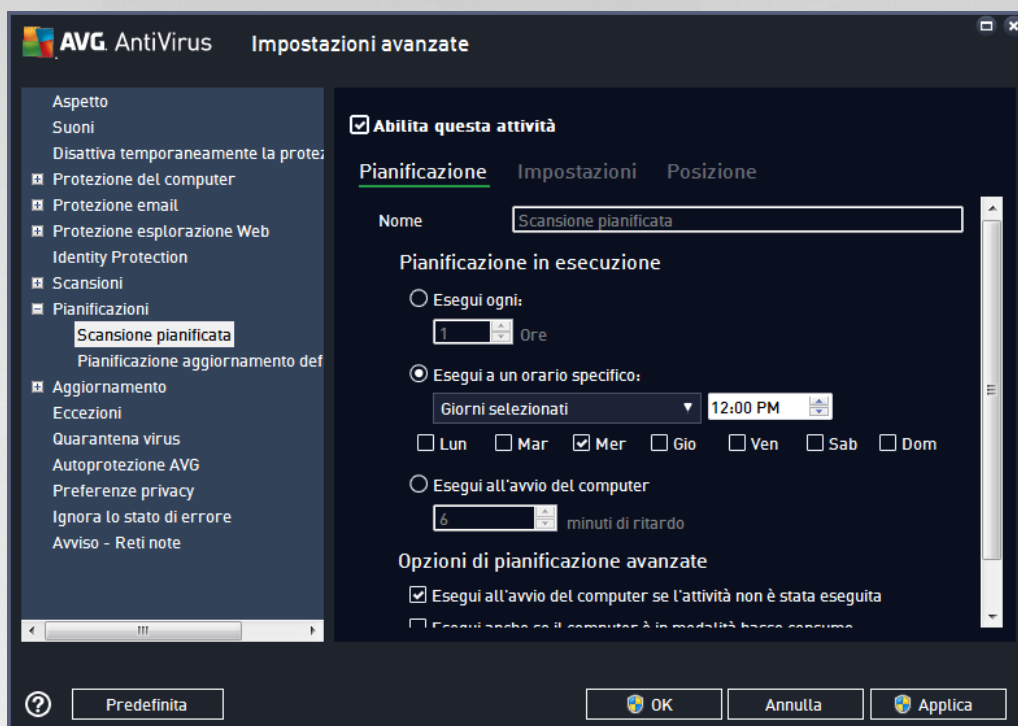
Nota: *per la descrizione di parametri specifici consultare il capitolo Impostazioni AVG avanzate / Scansione / Scansione intero computer.*

7.9. Pianificazioni

Nella sezione ***Pianificazioni*** è possibile modificare le impostazioni predefinite di:

- Scansione pianificata
- Pianificazione aggiornamento definizioni
- Pianificazione dell'aggiornamento del programma

7.9.1. Scansione pianificata

È possibile modificare i parametri della scansione pianificata (*o impostare una nuova pianificazione*) in tre schede. In ciascuna scheda è possibile selezionare/deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità:

Quindi, nel campo di testo **Nome** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma. Per le pianificazioni aggiunte successivamente (*è possibile aggiungere una nuova pianificazione facendo clic con il pulsante destro del mouse sulla voce **Scansione pianificata** nella struttura di esplorazione a sinistra*) è possibile specificare un nome personalizzato. In tal caso, il campo di testo sarà attivo per la modifica. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro.

Esempio: *non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via. Inoltre, non è necessario specificare nel nome della scansione se si tratta di una scansione dell'intero computer oppure relativa solo ai file o alle cartelle selezionati. Le scansioni saranno sempre una versione specifica della scansione dei file e delle cartelle selezionati.*

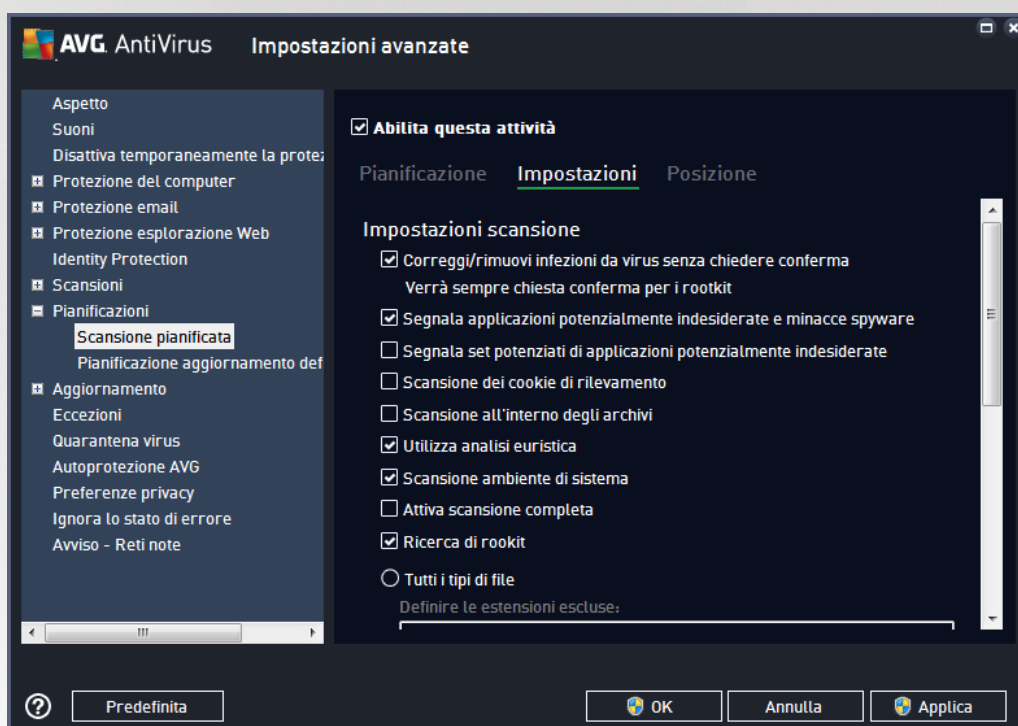
In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo (***Esegui ogni...***), specificando data e ora esatte (***Esegui a un orario specifico***), oppure definendo un evento a cui dovrà essere associato l'avvio della scansione (***Esegui all'avvio del computer***).

Opzioni di pianificazione avanzate

- ***Esegui all'avvio del computer se l'attività non è stata eseguita***: se si pianifica l'esecuzione dell'attività a un'ora specifica, questa opzione consentirà di verificare che la scansione venga eseguita in un momento successivo nel caso in cui il computer sia spento all'ora della pianificazione.

- ***Esegui anche se il computer è in modalità basso consumo***: consente di specificare se la scansione deve essere eseguita anche se il computer è in esecuzione con alimentazione a batteria all'orario pianificato.

Nella scheda ***Impostazioni*** è contenuto un elenco di parametri di scansione che possono essere attivati/ disattivati facoltativamente. Per impostazione predefinita, la maggior parte dei parametri è attivata e la funzionalità verrà applicata durante la scansione. ***A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita***:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita):* se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** *(attivata per impostazione predefinita):* selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** (*disattivata per impostazione predefinita*): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi

successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali i siti preferiti o il contenuto dei carrelli elettronici*).
- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.
- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.
- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.
- ***Attiva scansione completa*** (*disattivata per impostazione predefinita):* in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- ***Ricerca di rootkit*** *(attivata per impostazione predefinita):* la scansione Anti-Rootkit ricerca sul computer la presenza di eventuali rootkit (programmi e tecnologie in grado di coprire l'attività dei malware nel computer). Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Inoltre, è necessario decidere quali elementi sottoporre a scansione

- ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione (*dopo il salvataggio, le virgole vengono sostituite da punto e virgola*).
- ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.
- Facoltativamente, è possibile effettuare la ***Scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non si abbiano motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

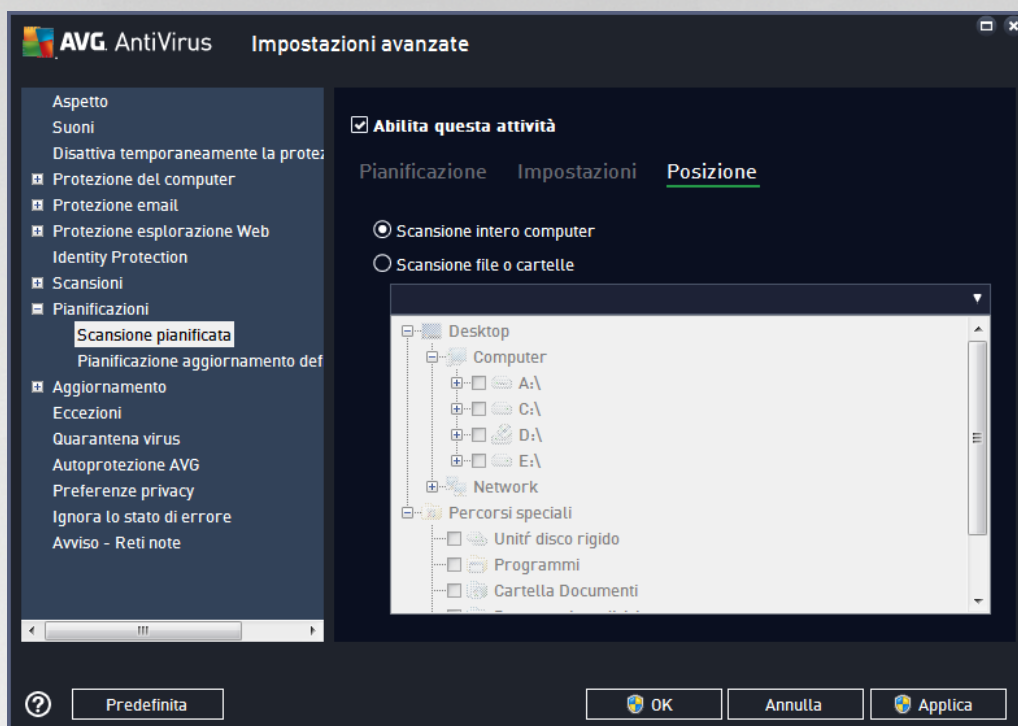
Regola la velocità di completamento della scansione

All'interno di questa sezione è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non in uso*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

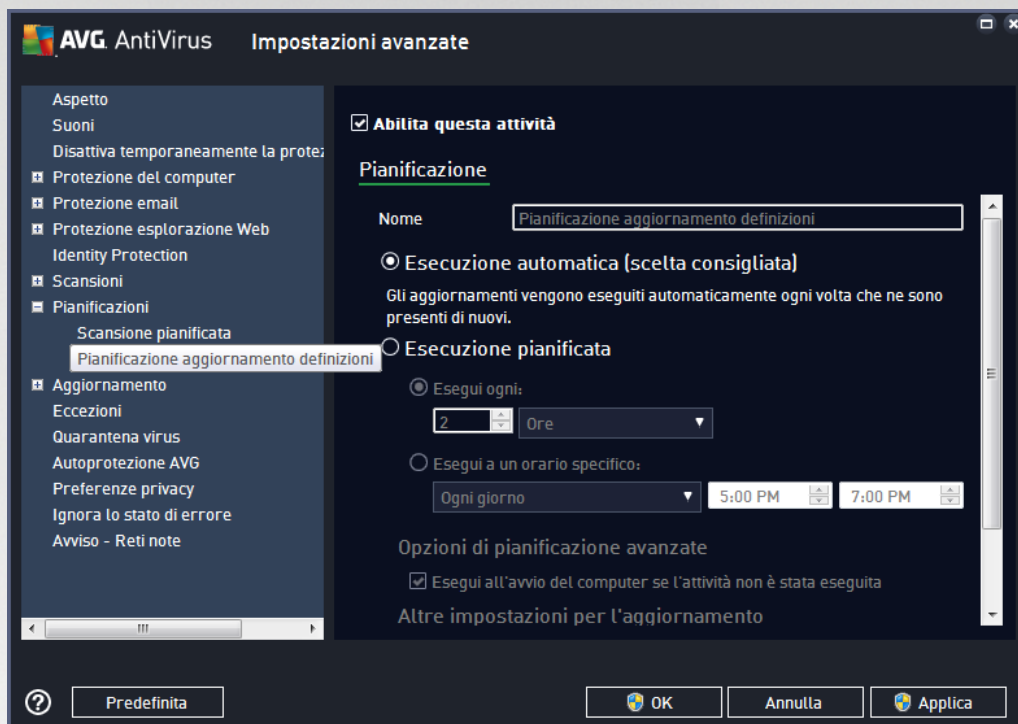
Imposta rapporti di scansione aggiuntivi

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

Opzioni arresto computer

Nella sezione ***Opzioni arresto computer***, è possibile decidere se il computer deve essere arrestato in modo automatico al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

Nella scheda ***Posizione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle. Se si seleziona la scansione di file o cartelle, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione.

7.9.2. Pianificazione aggiornamento definizioni

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento delle definizioni pianificato e attivarlo nuovamente in seguito:

In questa finestra di dialogo è possibile impostare alcuni parametri dettagliati della pianificazione dell'aggiornamento delle definizioni. Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Per impostazione predefinita, l'attività viene avviata in modo automatico (***Esegui automaticamente***) non appena è disponibile un nuovo aggiornamento delle definizioni dei virus. Si consiglia di non modificare questa configurazione, a meno che non sia assolutamente necessario. É inoltre possibile impostare l'esecuzione dell'attività manualmente, specificando gli intervalli di tempo per l'avvio del nuovo aggiornamento delle definizioni pianificato. È possibile definire l'ora tramite l'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (***Esegui ogni...***) oppure definendo data e ora esatte (***Esegui a un orario specifico***).

Opzioni di pianificazione avanzate

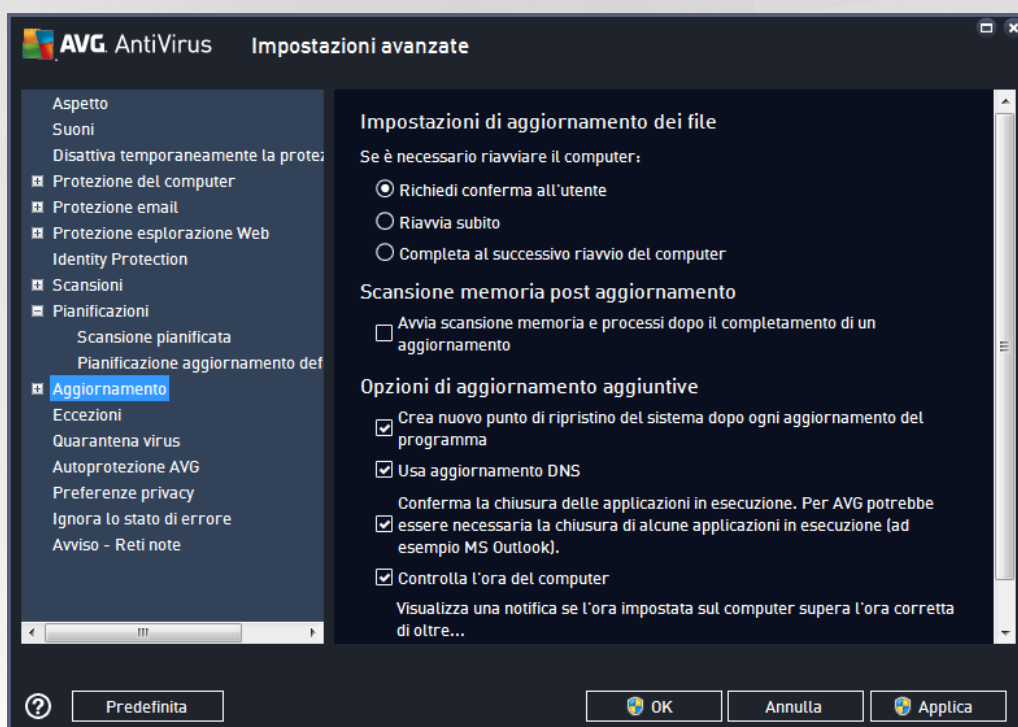
Questa sezione consente di definire le circostanze in cui deve essere avviato o non avviato l'aggiornamento se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni di aggiornamento

Infine, selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà***

disponibile per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando l'aggiornamento pianificato viene avviato in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona nella barra delle applicazioni di AVG (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

7.9.3. Pianificazione dell'aggiornamento del programma

Se ***realmente necessario***, è possibile deselezionare la voce ***Abilita questa attività*** per disattivare temporaneamente l'aggiornamento del programma pianificato e attivarlo nuovamente in seguito:

Nel campo di testo ***Nome*** (*disattivato per tutte le pianificazioni predefinite*) è presente il nome assegnato alla pianificazione in oggetto dal fornitore del programma.

Pianificazione in esecuzione

Consente di specificare gli intervalli di tempo per l'avvio del nuovo aggiornamento del programma pianificato. È possibile specificare l'ora dall'avvio ripetuto dell'aggiornamento dopo un certo periodo di tempo (***Esegui ogni***) o definendo data e ora esatte (***Esegui a un orario specifico***) oppure definendo un evento a cui dovrà essere associato l'avvio dell'aggiornamento (***Esegui all'avvio del computer***).

Opzioni di pianificazione avanzate

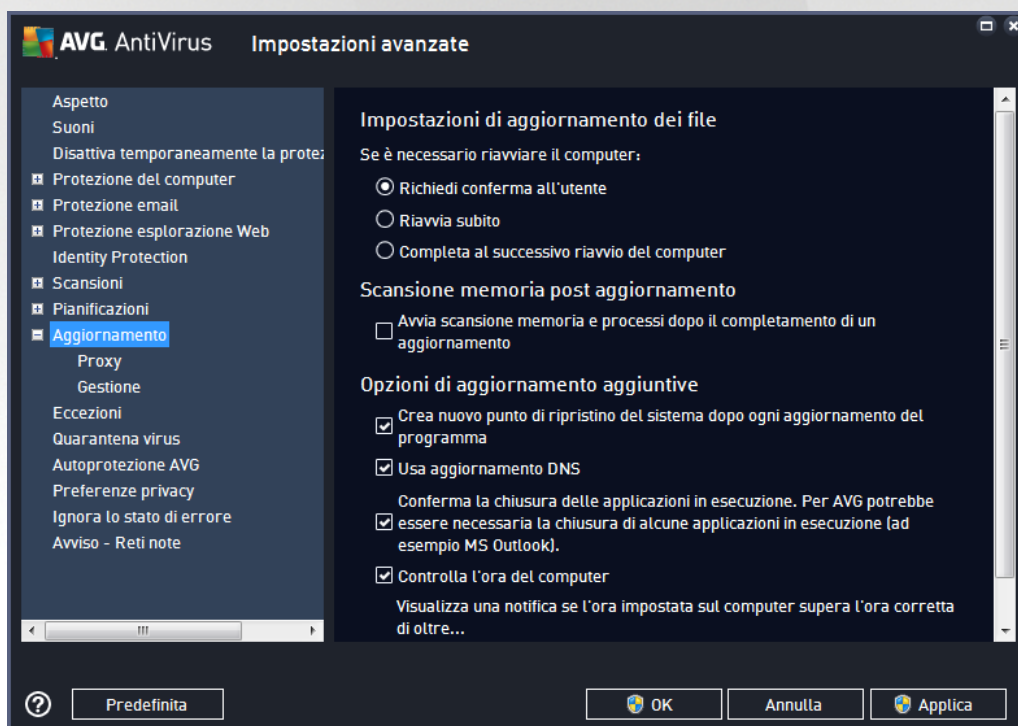
Questa sezione consente di definire le circostanze in cui deve o non deve essere avviato l'aggiornamento del programma se il computer si trova in modalità basso consumo oppure se è completamente spento.

Altre impostazioni per l'aggiornamento

Selezionare l'opzione ***Eseguire nuovamente l'aggiornamento quando la connessione Internet sarà disponibile*** per assicurarsi che, se la connessione Internet si interrompesse e il processo di aggiornamento non riuscisse, tale processo venga avviato di nuovo subito dopo il ripristino della connessione Internet. Quando l'aggiornamento pianificato viene avviato in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona della barra delle applicazioni di AVG (*a condizione che sia stata mantenuta la configurazione predefinita della finestra di dialogo Impostazioni avanzate/Aspetto*).

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta. In questo caso l'utente verrà informato del conflitto.*

7.10. Aggiornamento

La voce ***Aggiorna*** consente di aprire una finestra di dialogo in cui è possibile specificare i parametri generali relativi all'aggiornamento di AVG:

Quando eseguire l'aggiornamento dei file

In questa sezione è possibile effettuare la selezione tra tre diverse opzioni da utilizzare nel caso in cui il processo di aggiornamento richieda il riavvio del PC. È possibile pianificare la finalizzazione dell'aggiornamento per il successivo riavvio del PC oppure è possibile procedere subito al riavvio:

- ***Richiedi conferma dell'utente*** *(impostazione predefinita)*: verrà richiesto di approvare un riavvio del PC necessario per finalizzare il processo di aggiornamento

- ***Riavvia subito***: il computer verrà riavviato immediatamente in maniera automatica dopo la finalizzazione del processo di aggiornamento senza richiesta di conferma da parte dell'utente

- ***Completa al successivo riavvio del computer***: la finalizzazione del processo di aggiornamento verrà posticipata al successivo riavvio del computer. Tenere presente che questa opzione è consigliata solo se si è certi che il computer venga riavviato regolarmente, almeno una volta al giorno.

Scansione memoria post aggiornamento

Selezionare questa casella di controllo per specificare che si desidera avviare una nuova scansione della memoria al termine di ciascun aggiornamento. L'ultimo aggiornamento scaricato potrebbe contenere nuove definizioni dei virus e queste potrebbero applicarsi immediatamente alla scansione.

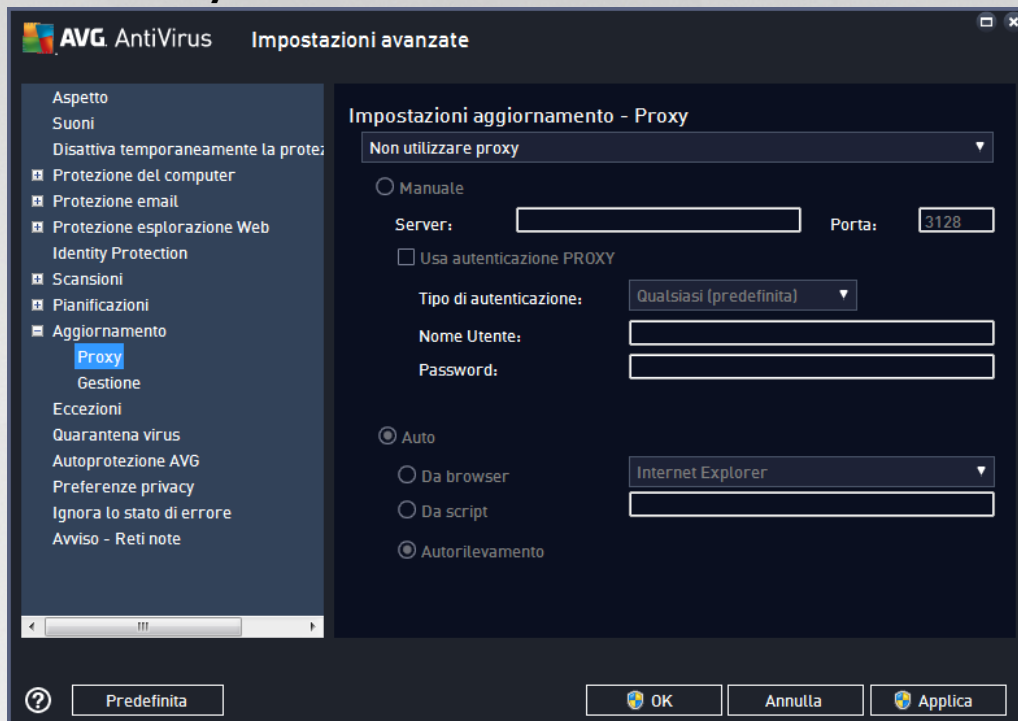
Opzioni di aggiornamento aggiuntive

- ***Crea nuovo punto di ripristino del sistema durante ogni aggiornamento del programma*** (*attivata per impostazione predefinita*): prima dell'avvio di ciascun aggiornamento del programma AVG viene creato un punto di ripristino del sistema. Se il processo di aggiornamento non ha esito positivo e il sistema operativo si blocca, è possibile ripristinare il sistema operativo nella configurazione originale da questo punto. Questa opzione è accessibile tramite Start / Tutti i programmi / Accessori / Utilità di sistema / Ripristino configurazione di sistema, tuttavia le eventuali modifiche sono consigliate ai soli utenti esperti. Mantenere selezionata questa casella di controllo se si desidera utilizzare questa funzionalità.

- ***Usa aggiornamento DNS*** (*attivata per impostazione predefinita*): con questa voce selezionata, una volta avviato l'aggiornamento, **AVG AntiVirus** ricerca informazioni sulla versione del database dei virus più recente e sulla versione del programma più recente sul server DNS. Quindi, solo i file di aggiornamento più piccoli e indispensabili vengono scaricati e applicati. In questo modo la quantità totale di dati scaricati viene ridotta al minimo e il processo di aggiornamento viene accelerato.

- ***Conferma la chiusura delle applicazioni in esecuzione*** (*attivata per impostazione predefinita*): questa opzione garantirà che nessuna applicazione in esecuzione venga chiusa senza autorizzazione, nel caso fosse necessario per la finalizzazione del processo di aggiornamento.

- ***Controlla l'ora del computer*** (*attivata per impostazione predefinita*): selezionare questa opzione per ricevere una notifica nel caso in cui l'ora del computer differisca dall'ora esatta di un valore superiore al numero di ore specificato.

7.10.1. Proxy

Il server proxy è un server autonomo o un servizio in esecuzione su un PC che garantisce una connessione più sicura a Internet. Secondo le regole di rete specificate è possibile accedere a Internet direttamente o tramite il server proxy. Sono anche consentite entrambe le possibilità contemporaneamente. Quindi, nella prima voce della finestra di dialogo ***Impostazioni aggiornamento – Proxy*** è necessario selezionare l'opzione desiderata dal menu della casella combinata:

- ***Non utilizzare proxy***: impostazioni predefinite
- ***Utilizza proxy***
- ***Tenta la connessione utilizzando il proxy e, se non riesce, esegui la connessione direttamente***

Se si seleziona un'opzione utilizzando un server proxy, sarà necessario specificare ulteriori dati. Le impostazioni del server possono essere configurate manualmente o automaticamente.

Configurazione manuale

Se si seleziona la configurazione manuale (selezionare *l'opzione* ***Manuale*** *per attivare la sezione della finestra di dialogo corrispondente*) è necessario specificare le seguenti voci:

- ***Server***: specificare l'indirizzo IP o il nome del server
- ***Porta***: specifica il numero della porta che consente l'accesso a Internet (*per impostazione predefinita, il numero è impostato su 3128 ma può essere modificato; se non si è sicuri, contattare l'amministratore di rete*)

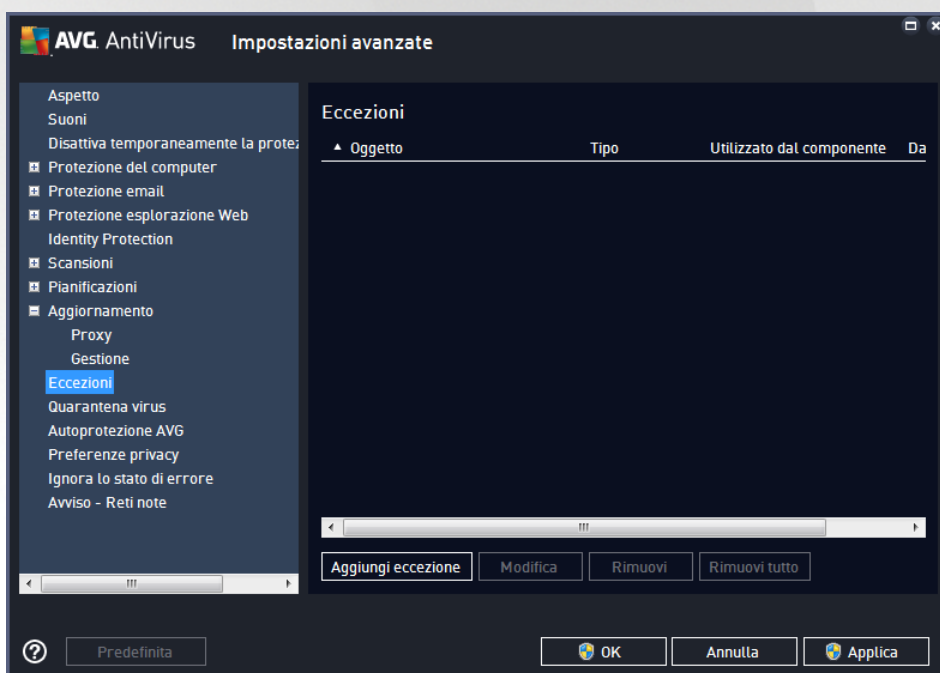
È anche possibile che sul server proxy siano state configurate regole specifiche per ciascun utente. Se il server proxy è impostato in questo modo, selezionare l'opzione ***Usa autenticazione PROXY*** per verificare che nome utente e password siano validi per la connessione a Internet tramite il server proxy.

Configurazione automatica

Se si seleziona la configurazione automatica *(selezionare l'opzione **Auto** per attivare la sezione della finestra di dialogo corrispondente*), selezionare quindi l'origine della configurazione proxy:

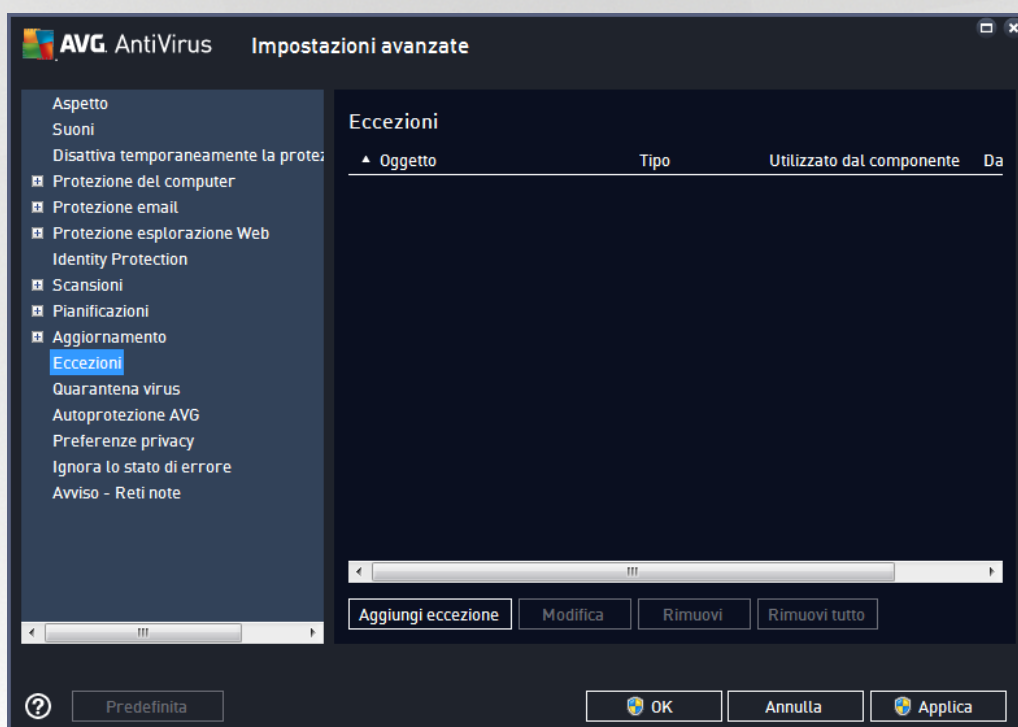
- ***Da browser***: la configurazione verrà letta dal browser Internet predefinito
- ***Da script***: la configurazione verrà letta da uno script scaricato con la funzione di restituzione dell'indirizzo proxy
- ***Autorilevamento***: la configurazione verrà rilevata automaticamente direttamente dal server proxy

7.10.2. Gestione

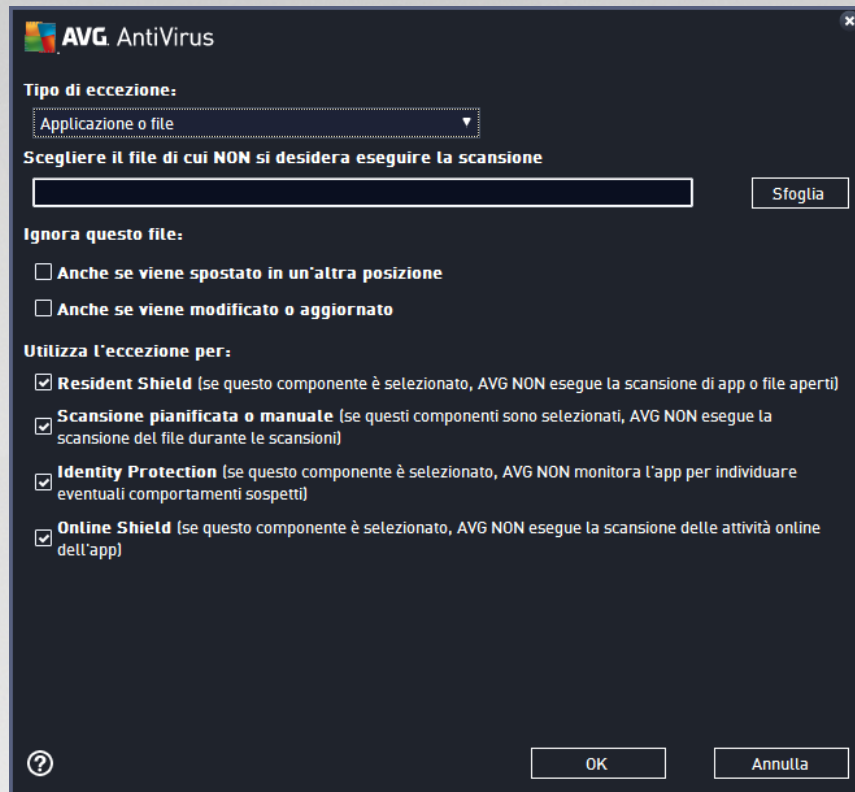
La finestra di dialogo ***Gestione aggiornamenti*** offre due opzioni accessibili tramite due pulsanti:

- ***Elimina file di aggiornamento temporanei***: selezionare questo pulsante per eliminare tutti i file di aggiornamento ridondanti dal disco rigido (*per impostazione predefinita, questi file restano memorizzati per 30 giorni*)
- ***Ripristina la precedente versione del database dei virus***: selezionare questo pulsante per eliminare l'ultima versione del database dei virus dal disco rigido e tornare alla precedente versione salvata (*la nuova versione del database dei virus verrà inserita nel successivo aggiornamento*)

7.11. Eccezioni

Nella finestra di dialogo ***Eccezioni*** è possibile definire le eccezioni, ovvero voci che verranno ignorate da **AVG AntiVirus**. In genere, sarà necessario definire un'eccezione se AVG continua a rilevare un programma o un file come se fosse una minaccia oppure blocca un sito Web sicuro come se fosse pericoloso. Se si aggiungono tali file o siti Web a questo elenco eccezioni, AVG non li segnalerà né bloccherà più.

Assicurarsi sempre che il file, il programma o il sito Web in questione sia davvero completamente sicuro.

Nel grafico della finestra di dialogo viene visualizzato un elenco di eccezioni, se sono già state definite. Accanto a ogni elemento è presente una casella di controllo. Se la casella di controllo è selezionata, l'eccezione è attiva. In caso contrario, è semplicemente definita ma non utilizzata. Facendo clic su un'intestazione di colonna, è possibile ordinare gli elementi consentiti in base al criterio corrispondente.

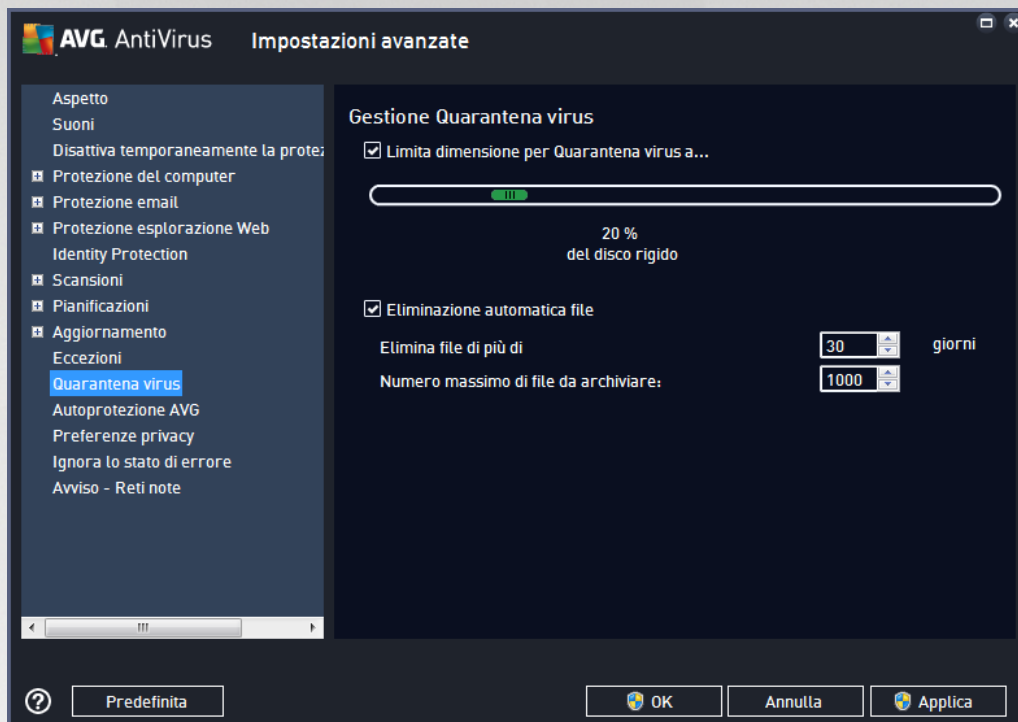
Pulsanti di controllo

- ***Aggiungi eccezione***: fare clic per aprire una nuova finestra di dialogo in cui è possibile specificare la voce che deve essere esclusa dalla scansione AVG.

Prima di tutto, verrà richiesto di definire il tipo di oggetto, ovvero se si tratta di un'applicazione, un file, una cartella, un URL o un certificato. Quindi sarà necessario specificare il percorso del relativo oggetto nel disco o digitare l'URL. Infine, è possibile selezionare quali funzionalità AVG devono ignorare l'oggetto selezionato *(Resident Shield, Identity Protection, Scansione)*.

- ***Modifica***: questo pulsante è attivo solo se alcune eccezioni sono state già definite e inserite nell'elenco. È quindi possibile utilizzare il pulsante per aprire la finestra di modifica relativa all'eccezione selezionata e configurare i parametri dell'eccezione.

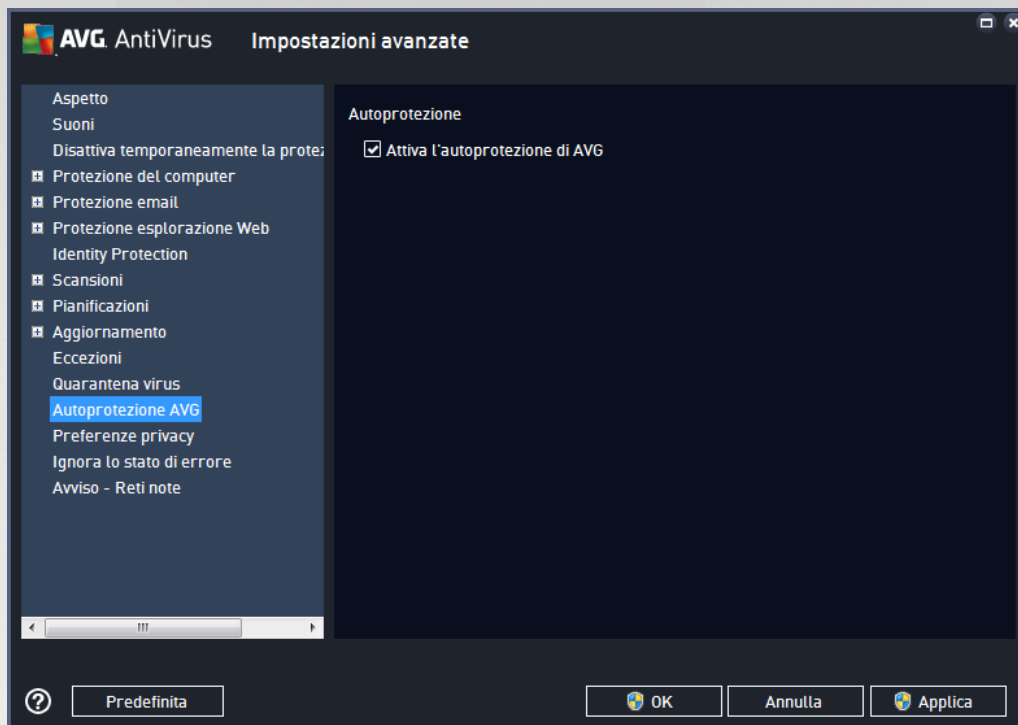
- ***Rimuovi***: questo pulsante consente di annullare un'eccezione definita in precedenza. È possibile rimuovere le eccezioni una per una o evidenziare un blocco nell'elenco e annullare le eccezioni definite. Dopo aver annullato l'eccezione, il file, la cartella o l'URL relativi verranno controllati di nuovo da AVG. Tenere presente che verrà rimossa solo l'eccezione, non il relativo file o cartella.

- ***Rimuovi tutte***: utilizzare questo pulsante per eliminare tutte le eccezioni definite nell'elenco.

7.12. Quarantena virus

La finestra di dialogo ***Gestione Quarantena virus*** consente di definire diversi parametri relativi alla gestione degli oggetti archiviati in Quarantena virus:

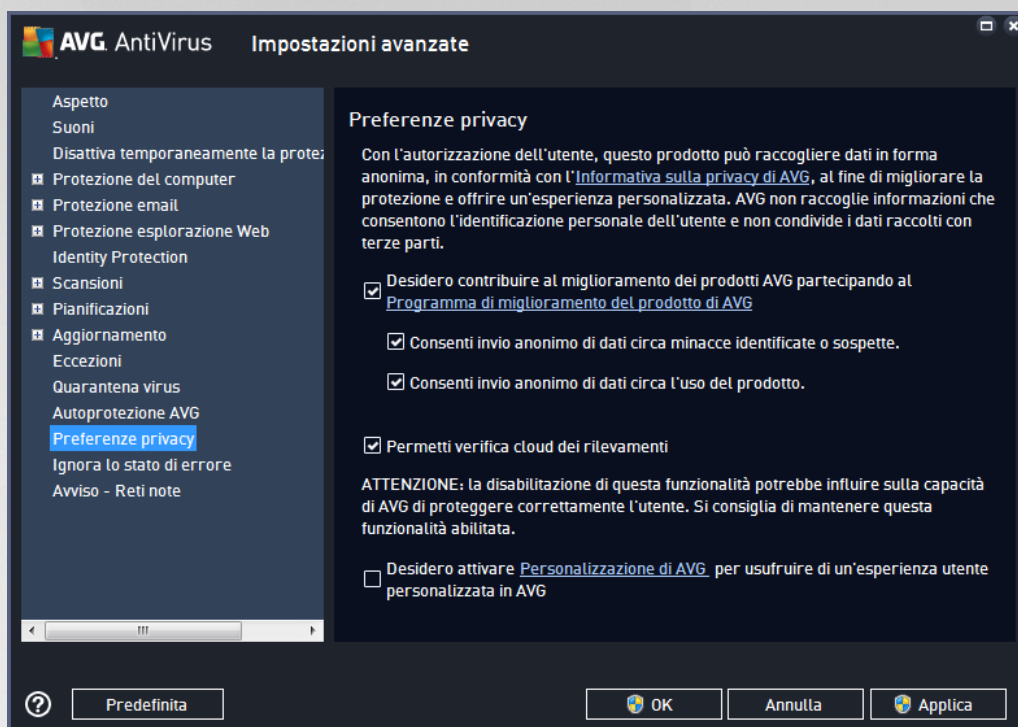
- ***Limite dimensione per Quarantena virus***: utilizzare il dispositivo di scorrimento per impostare la dimensione massima di Quarantena virus. La dimensione è specificata in maniera proporzionale rispetto alla dimensione del disco locale.

- ***Eliminazione automatica file***: questa sezione consente di definire la durata massima di memorizzazione degli oggetti in Quarantena virus (***Elimina file di più di...giorni***) e il numero massimo di file da memorizzare in Quarantena virus (***Numero massimo di file da memorizzare***).

7.13. Autoprotezione di AVG

Autoprotezione di AVG consente a **AVG AntiVirus** di proteggere i relativi processi, file, chiavi di registro e driver da modifiche o disattivazioni. Il motivo principale per cui si utilizza questo tipo di protezione è che alcune minacce sofisticate tentano di disattivare la protezione antivirus per causare liberamente danni al computer.

Si consiglia di mantenere questa funzionalità attivata!

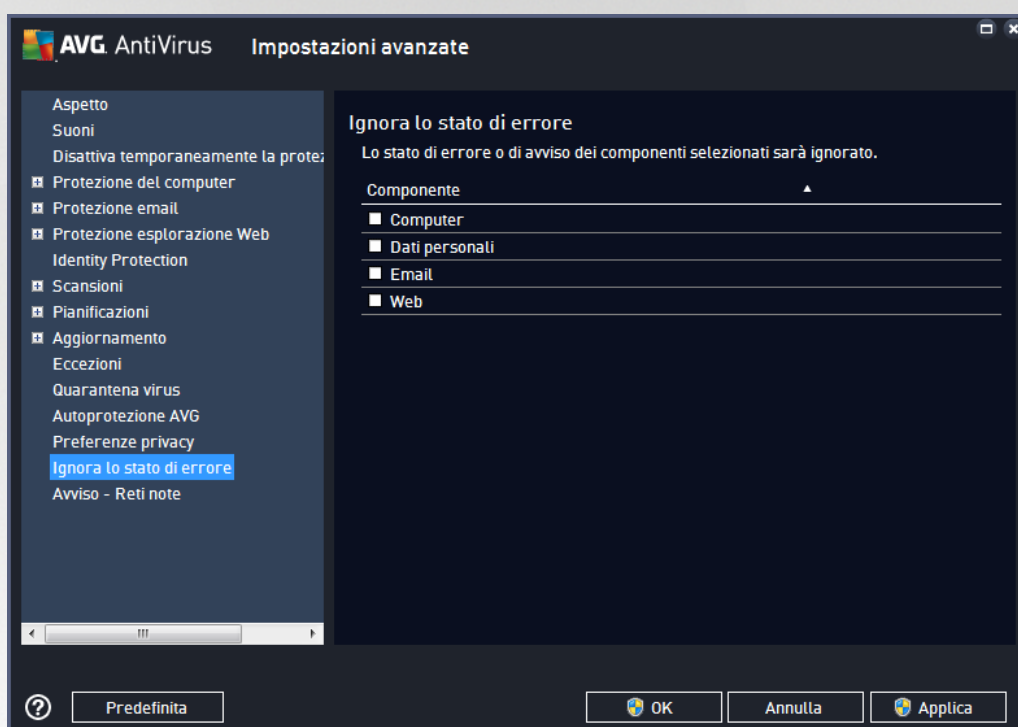
7.14. Preferenze privacy

La finestra di dialogo ***Preferenze privacy*** invita l'utente a partecipare al programma per il miglioramento del prodotto AVG per aiutarci ad aumentare il livello di protezione generale in Internet. La segnalazione ci consente di raccogliere informazioni aggiornate sulle minacce più recenti da tutti gli utenti a livello mondiale e di migliorare la protezione per tutti. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente. Nei rapporti non vengono inclusi dati personali. La segnalazione delle minacce rilevate è opzionale. Tuttavia si consiglia si mantenere attivata questa opzione. La segnalazione ci aiuta a migliorare la protezione per tutti gli utenti AVG.

Nella finestra di dialogo sono disponibili le seguenti opzioni di impostazione:

- ***Desidero contribuire al miglioramento dei prodotti AVG partecipando al Programma di miglioramento del prodotto AVG*** *(attivata per impostazione predefinita)*: per aiutarci a migliorare ulteriormente **AVG AntiVirus**, mantenere selezionata questa casella di controllo. Ciò consentirà di segnalare ad AVG tutte le minacce riscontrate. In questo modo saremo in grado di raccogliere informazioni aggiornate sui malware da tutti gli utenti a livello mondiale per offrire un livello di protezione ancora superiore. La segnalazione viene elaborata automaticamente, pertanto non provoca alcun disturbo all'utente e nei rapporti non vengono inclusi dati personali.
    - ***Consenti invio dopo conferma dell'utente di dati circa email identificate erroneamente*** *(attiva per impostazione predefinita)*: invia informazioni sui messaggi email identificati erroneamente come spam o sui messaggi di spam non rilevati dal servizio Anti-Spam. Per l'invio di questo tipo di informazioni verrà richiesta la conferma dell'utente.
    - ***Consenti invio anonimo di dati circa minacce identificate o sospette*** *(attiva per impostazione predefinita)*: invia informazioni su comportamenti o codici sicuramente pericolosi o sospetti *(può trattarsi di un virus, uno spyware o una pagina Web dannosa a cui si sta tentando di accedere) rilevati nel computer.*
    - ***Consenti invio anonimo di dati circa l'uso del prodotto*** *(attiva per impostazione predefinita)*: invia statistiche di base sull'uso dell'applicazione, ad esempio numero di rilevamenti, scansioni avviate, aggiornamenti riusciti/non riusciti e così via.
- ***Permetti verifica cloud dei rilevamenti*** *(attiva per impostazione predefinita)*: le minacce rilevate verranno controllate per verificare l'effettiva presenza di infezioni, in modo da evitare i falsi positivi.
- ***Desidero attivare Personalizzazione di AVG per usufruire di un'esperienza utente personalizzata in AVG*** *(disattivata per impostazione predefinita)*: questa funzionalità analizza in

modo anonimo il comportamento dei programmi e delle applicazioni installati nel PC. Grazie a questa analisi, AVG può offrire servizi personalizzati in base alle specifiche esigenze, per assicurare la massima protezione.

7.15. Ignora lo stato di errore

Nella finestra di dialogo ***Ignora lo stato di errore*** è possibile selezionare i componenti in merito ai quali non si desidera ricevere informazioni:

Per impostazione predefinita, in questo elenco non è selezionato alcun componente. Ciò significa che se per un qualsiasi componente si verifica uno stato di errore, se ne verrà immediatamente informati tramite:

- l'icona presente nella barra delle applicazioni: quando tutte le parti di AVG funzionano correttamente, l'icona viene visualizzata in quattro colori; se si verifica un errore, l'icona viene visualizzata con un punto esclamativo giallo,

- una descrizione del problema esistente visualizzata nella sezione Informazioni sullo stato di protezione della finestra principale di AVG

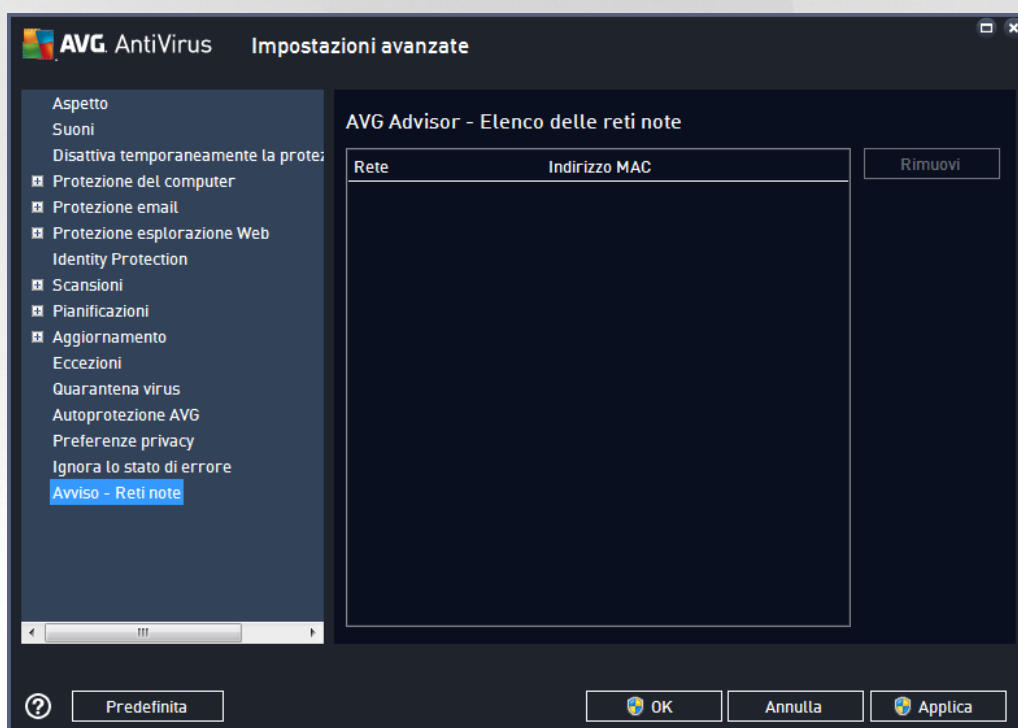
Potrebbe verificarsi una situazione in cui, per qualsiasi motivo, risulti necessario disattivare un componente temporaneamente. ***Questa operazione tuttavia non è consigliabile, si dovrebbe tentare di mantenere attivati tutti i componenti in modo permanente e con la configurazione predefinita***. Ma nel caso si verifichi questa situazione, l'icona presente nella barra delle applicazioni segnala automaticamente lo stato di errore del componente. In casi del genere, tuttavia, non è possibile parlare di errore effettivo, poiché la condizione è stata indotta deliberatamente dall'utente e si è consapevoli del potenziale rischio. Nel contempo, una volta che viene visualizzata in grigio, l'icona non può più segnalare eventuali errori ulteriori che potrebbero verificarsi.

Per gestire situazioni simili, all'interno della finestra di dialogo ***Ignora lo stato di errore*** è possibile selezionare

i componenti che potrebbero trovarsi in stato di errore (*o disattivati*) in merito ai quali non si desidera ricevere informazioni. Selezionare il pulsante ***OK*** per confermare.

7.16. Avviso - Reti note

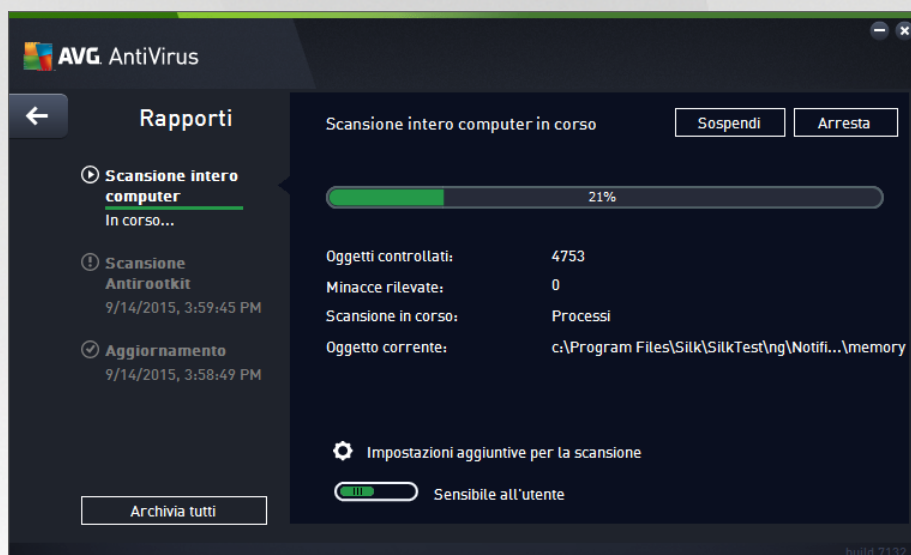
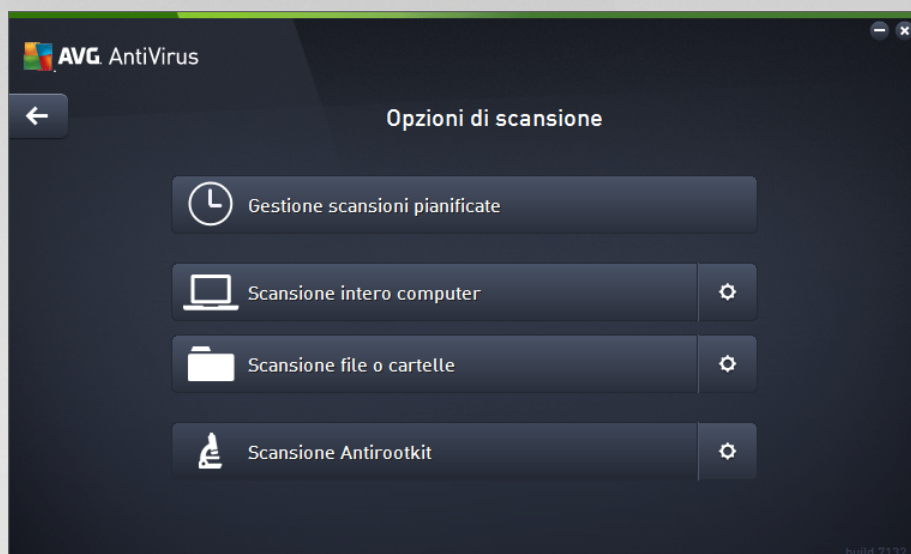
In AVG Advisor è inclusa una funzionalità che monitora le reti a cui si esegue la connessione e, se viene rilevata una nuova rete *(con un nome di rete già utilizzato, che potrebbe generare confusione)*, visualizza una notifica e suggerisce di verificare la sicurezza della rete. Se si considera sicura la nuova rete, è possibile salvarla in questo elenco *(tramite il collegamento fornito nella notifica di AVG Advisor che scorre sulla barra delle applicazioni quando viene rilevata una rete sconosciuta. Per ulteriori dettagli vedere il capitolo su AVG Advisor)*. AVG Advisor memorizzerà gli attributi univoci della rete *(in particolare l'indirizzo MAC)* e in seguito non visualizzerà la notifica. Ogni rete a cui si esegue la connessione verrà automaticamente considerata come rete conosciuta e aggiunta all'elenco. È possibile eliminare singole voci facendo clic sul pulsante ***Rimuovi***: la rete corrispondente verrà nuovamente considerata sconosciuta e potenzialmente non sicura.

In questa finestra di dialogo è possibile controllare quali reti sono considerate conosciute:

Nota: *la funzione reti conosciute in AVG Advisor non è supportata in Windows XP a 64 bit.*

8. Scansione AVG

Per impostazione predefinita, **AVG AntiVirus** non esegue alcuna scansione, poiché dopo la scansione iniziale *(che all'utente viene richiesto di avviare)*, il computer dovrebbe essere perfettamente protetto dai componenti permanenti di **AVG AntiVirus** che sono sempre attivi e non lasciano entrare codice dannoso nel sistema. Naturalmente, è possibile pianificare l'esecuzione di una scansione a intervalli regolari o avviare manualmente una scansione in qualsiasi momento in base alle esigenze.

L'interfaccia di scansione di AVG è accessibile dall'interfaccia utente principale tramite il pulsantesuddiviso graficamente in due sezioni:

- ***Esegui scansione***: fare clic su questo pulsante per avviare la Scansione intero computer e visualizzare l'avanzamento e i relativi risultati nella finestra Rapporti, che viene aperta automaticamente:

- ***Opzioni***: fare clic su questo pulsante *(visualizzato graficamente come tre linee orizzontali su sfondo verde)* per aprire la finestra di dialogo ***Opzioni di scansione***, dove è possibile gestire le scansioni pianificate e modificare i parametri di Scansione intero computer / Scansione file o cartelle.

Nella finestra di dialogo ***Opzioni di scansione*** sono disponibili tre sezioni principali per la configurazione delle scansioni:

- ***Gestione scansioni pianificate***: fare clic su questa opzione per aprire una nuova finestra di dialogo con una panoramica di tutte le scansioni pianificate. Se non sono state definite scansioni personalizzate, nell'elenco sarà visualizzata solo una scansione pianificata predefinita dal fornitore del software. Per impostazione predefinita, tale scansione è disattivata. Per attivarla, fare clic con il pulsante destro del mouse sull'opzione *Abilita attività* dal menu di scelta rapida. Dopo aver abilitato la scansione pianificata, è possibile modificarne la configurazione utilizzando il pulsante *Modifica pianificazione scansione*. Inoltre, è possibile fare clic sul pulsante *Aggiungi scansione pianificata* per creare e pianificare una scansione personalizzata.

- ***Scansione intero computer / Impostazioni***: questo pulsante è suddiviso in due sezioni. Fare clic sull'opzione *Scansione intero computer* per avviare immediatamente la scansione dell'intero computer *(per ulteriori dettagli, vedere il capitolo Scansioni predefinite / Scansione intero computer)*. Facendo clic sulla sezione *Impostazioni* è possibile accedere alla finestra di dialogo di configurazione della scansione intero computer.

- ***Scansione file o cartelle / Impostazioni***: anche questo pulsante è suddiviso in due sezioni. Fare clic sull'opzione *Scansione file o cartelle* per avviare immediatamente la scansione delle aree selezionate del computer *(per ulteriori dettagli, vedere il capitolo Scansioni predefinite / Scansione file o cartelle)*. Facendo clic sulla sezione *Impostazioni* è possibile accedere alla finestra di dialogo di configurazione della scansione file o cartelle.

- ***Esegui la ricerca di rootkit nel computer / Impostazioni***: fare clic sulla sezione di sinistra del pulsante denominata *Esegui la ricerca di rootkit nel computer* per avviare immediatamente la ricerca di rootkit *(per ulteriori dettagli, vedere il capitolo Scansioni predefinite / Esegui la ricerca di rootkit nel computer)*. Facendo clic sulla sezione *Impostazioni* è possibile accedere alla finestra di dialogo di configurazione della ricerca di rootkit.

8.1. Scansioni predefinite

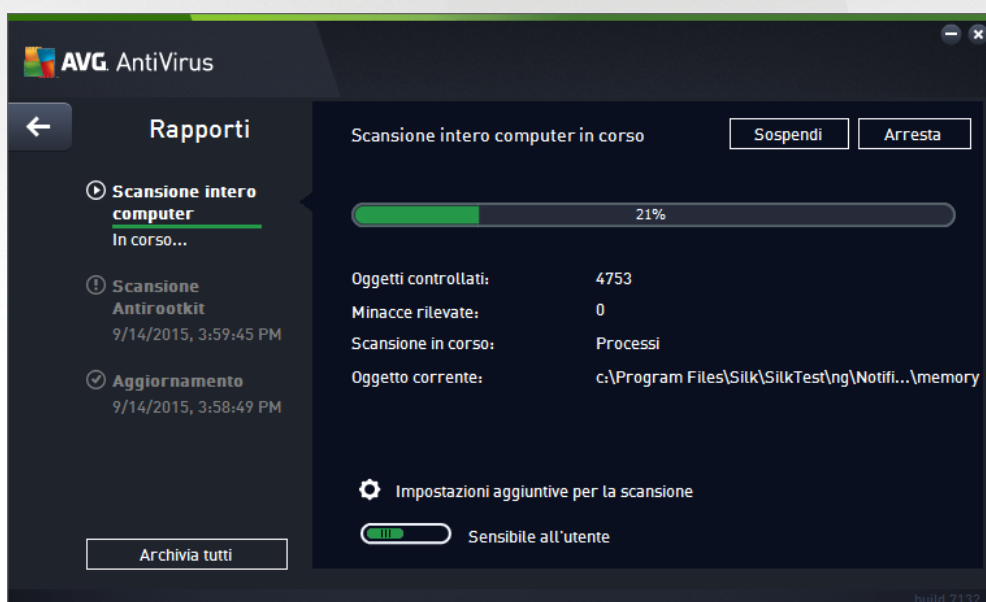
Una delle funzioni principali di **AVG AntiVirus** è la scansione su richiesta. I controlli su richiesta sono progettati per eseguire la scansione di varie parti del computer quando si sospetta una possibile infezione da virus. Comunque, si consiglia di eseguire regolarmente tali verifiche anche se non si ritiene che siano presenti virus nel computer.

In **AVG AntiVirus** sono disponibili i seguenti tipi di scansione predefiniti dal fornitore del software:

8.1.1. Scansione intero computer

Scansione intero computer consente di eseguire scansioni dell'intero computer per il rilevamento di possibili infezioni e/o di applicazioni potenzialmente indesiderate. Questo controllo eseguirà la scansione di tutti i dischi rigidi nel computer, rileverà e correggerà i virus trovati oppure sposterà l'infezione rilevata in Quarantena virus. È necessario pianificare la scansione dell'intero computer almeno una volta la settimana.

Avvio della scansione

La ***Scansione intero computer*** può essere avviata direttamente dall'interfaccia utente principale facendo clic sul pulsante ***Esegui scansione***. Non è necessario configurare ulteriori impostazioni specifiche per questo tipo di scansione. La scansione verrà avviata immediatamente. Nella finestra di dialogo ***Scansione intero computer in corso*** (*vedere la schermata*) è possibile controllare l'avanzamento della scansione e i relativi risultati. La scansione può essere temporaneamente interrotta (***Sospendi***) oppure annullata (***Arresta***) se necessario.

Modifica della configurazione della scansione

È possibile modificare la configurazione di ***Scansione intero computer*** nella finestra di dialogo ***Scansione intero computer – Impostazioni*** *(tale finestra è accessibile tramite il collegamento Impostazioni per Scansione intero computer nella finestra Opzioni di scansione).* ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

Nell'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita)*: se viene identificato un virus durante la scansione, può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** *(attivata per impostazione predefinita)*: selezionare questa casella di controllo per attivare la scansione per ricercare sia spyware che virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** *(disattivata per impostazione predefinita)*: selezionare questa casella di controllo per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** *(disattivata per impostazione predefinita)*: questo parametro specifica che i cookie devono essere rilevati *(i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici)*.

- ***Scansione all'interno degli archivi*** *(disattivata per impostazione predefinita)*: questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.

- ***Usa analisi euristiche*** *(attivata per impostazione predefinita)*: l'analisi euristica *(emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale)* sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** *(attivata per impostazione predefinita)*: la scansione verrà eseguita anche sulle aree di sistema del computer.
- ***Attiva scansione completa*** *(disattivata per impostazione predefinita)*: in situazioni specifiche *(se si sospetta che il computer sia stato infettato)* per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.
- ***Ricerca di rootkit*** *(attivata per impostazione predefinita)*: include la scansione Antirootkit nella scansione dell'intero computer. È anche possibile avviare la Scansione Antirootkit separatamente.
- ***Impostazioni di scansione aggiuntive*** : il collegamento consente di aprire una nuova finestra di dialogo Impostazioni di scansione aggiuntive in cui è possibile specificare i parametri descritti di seguito.

- o ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).
- o ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:
  - ➢ ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione.
  - ➢ ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di*

scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

- Facoltativamente, è possibile effettuare la ***scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer indipendentemente dalla durata della scansione*) o più velocemente con utilizzo delle risorse di sistema più elevato (*utile ad esempio quando ci si allontana temporaneamente dal computer*).

- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti selezionare:

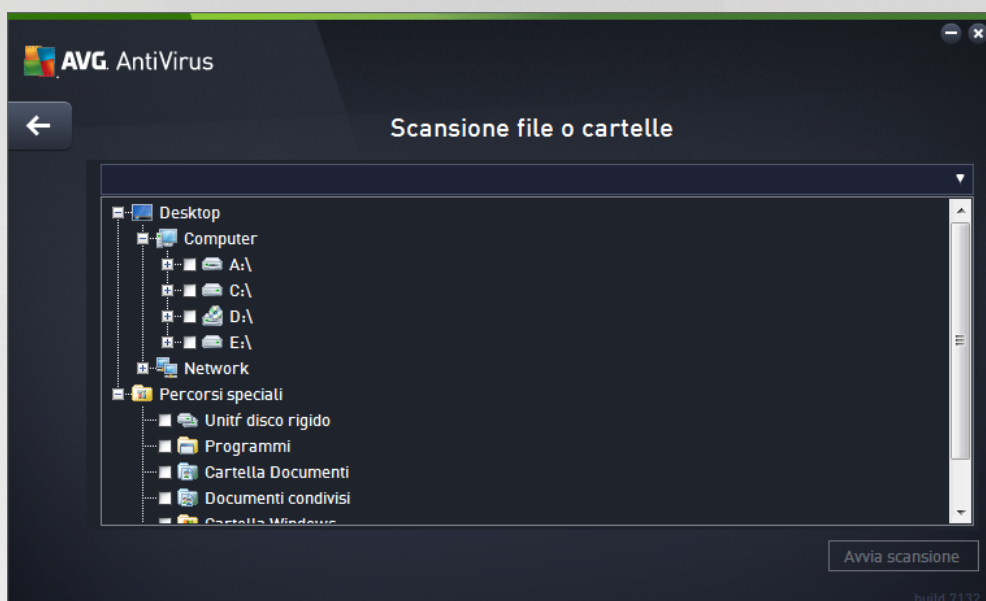
Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione, definita come descritto nel capitolo Scansione AVG / Pianificazione di scansioni / Scansione da eseguire. Se si decide di modificare la configurazione predefinita di* ***Scansione intero computer****, è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni dell'intero computer.*

8.1.2. Scansione file o cartelle

Scansione file o cartelle: consente di eseguire solamente la scansione delle aree del computer selezionate (specifici *dischi rigidi, dischi floppy, CD, cartelle e così via*). L'avanzamento della scansione nel caso di rilevamento di virus e relativo trattamento è uguale a quello della scansione dell'intero computer: gli eventuali virus rilevati vengono corretti o spostati in Quarantena virus. La scansione di file o cartelle specifiche può essere utilizzata per impostare controlli personalizzati e la relativa pianificazione in base alle esigenze.

Avvio della scansione

È possibile avviare la ***Scansione file o cartelle*** direttamente dalla finestra di dialogo Opzioni di scansione facendo clic sul pulsante **Scansione file o cartelle**. Viene aperta una nuova finestra di dialogo ***Selezionare file o cartelle specifiche per la scansione***. Nella struttura del computer selezionare le cartelle da sottoporre a scansione. Il percorso di ciascuna cartella selezionata verrà generato automaticamente e visualizzato nella

casella di testo nella parte superiore della finestra di dialogo. È inoltre possibile sottoporre a scansione una specifica cartella escludendo tutte le relative sottocartelle, a questo scopo scrivere un segno meno "**-**" all'inizio del percorso generato automaticamente (*vedere la schermata*). Per escludere l'intera cartella dalla scansione, utilizzare il parametro "**!**". Infine, per avviare la scansione, selezionare il pulsante ***Avvia scansione***. Il processo di scansione è praticamente identico a quello di Scansione intero computer.

Modifica della configurazione della scansione

È possibile modificare la configurazione di ***Scansione file o cartelle*** nella finestra di dialogo ***Scansione file o cartelle – Impostazioni*** *(tale finestra è accessibile tramite il collegamento Impostazioni per Scansione file o cartelle nella finestra Opzioni di scansione). **Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

Nell'elenco dei parametri di scansione è possibile attivare/disattivare parametri specifici in base alle esigenze:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita)*: Se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto infetto verrà spostato in Quarantena virus.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** *(attivata per impostazione predefinita)*: Selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** *(disattivata per impostazione predefinita)*: Selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** *(disattivata per impostazione predefinita)*: Questo parametro specifica che i cookie devono essere rilevati *(i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali le preferenze dei siti o il contenuto dei carrelli elettronici)*.

- ***Scansione all'interno degli archivi*** *(attivata per impostazione predefinita)*: Questo parametro specifica che la scansione deve controllare tutti i file inclusi all'interno di un archivio, quali ZIP, RAR e così via.

- ***Usa analisi euristiche*** *(attivata per impostazione predefinita)*: l'analisi euristica *(emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale)* sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** *(disattivata per impostazione predefinita)*: la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** *(disattivata per impostazione predefinita)*: in situazioni specifiche *(se si sospetta che il computer sia stato infettato)* per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Impostazioni di scansione aggiuntive***: il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione (***Arresta computer al completamento della scansione***), viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato (***Forza arresto se il computer è bloccato***).

- ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione.

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili (*i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili*), inclusi i file multimediali (*file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili dai virus*). Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile effettuare la ***scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non siano presenti motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

- ***Regola la velocità di completamento della scansione***: è possibile utilizzare il dispositivo di scorrimento per modificare la priorità del processo di scansione. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. In alternativa, è possibile eseguire il processo di scansione più lentamente in modo da ridurre al minimo il carico sulle risorse di sistema (*utile quando è necessario lavorare al computer indipendentemente dalla durata della scansione*) o più velocemente con un utilizzo delle risorse di sistema più elevato (*utile ad esempio quando ci si allontana temporaneamente dal computer*).

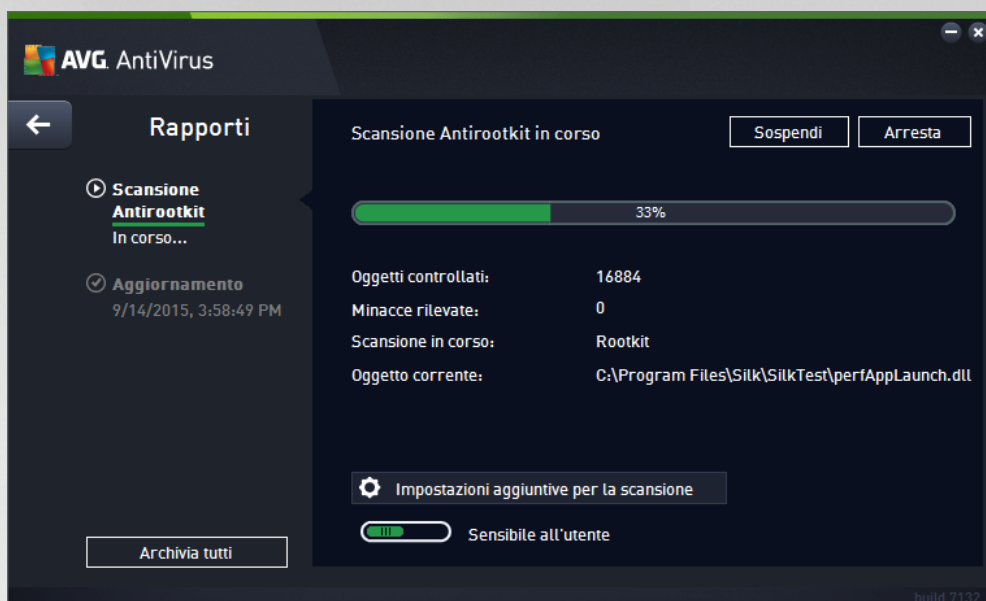
- ***Imposta rapporti di scansione aggiuntivi***: il collegamento consente di aprire una nuova finestra di dialogo ***Rapporti di scansione*** in cui è possibile selezionare quali tipi di rilevamenti segnalare:

Avviso: *queste impostazioni di scansione sono identiche ai parametri di una nuova scansione, definita come descritto nel capitolo Scansione AVG / Pianificazione di scansioni / Scansione da eseguire. Se si decide di modificare la configurazione predefinita di* ***Scansione file o cartelle*** *è possibile salvare le nuove impostazioni come configurazione predefinita da utilizzare per tutte le altre scansioni di file o cartelle specifiche. Inoltre, questa configurazione verrà utilizzata come modello per tutte le nuove scansioni pianificate (tutte le scansioni personalizzate si basano sulla configurazione corrente di Scansione file o cartelle).*

8.1.3. Esegui la ricerca di rootkit nel computer

Esegui la ricerca di rootkit nel computer consente di rilevare e rimuovere efficacemente i rootkit dannosi, ovvero programmi e tecnologie che possono camuffare la presenza di software dannoso nel computer. Un rootkit è progettato per assumere il controllo di base di un sistema senza autorizzazione da parte dei proprietari e dei gestori legittimi del sistema. La scansione è in grado di rilevare i rootkit in base a un gruppo predefinito di regole. Se viene individuato un rootkit, non significa necessariamente che sia infetto. Talvolta i rootkit vengono utilizzati come driver o fanno parte di applicazioni regolari.

Avvio della scansione

Esegui la ricerca di rootkit nel computer può essere avviato direttamente dalla finestra di dialogo Opzioni di scansione facendo clic sul pulsante ***Esegui la ricerca di rootkit nel computer***. Verrà aperta una nuova finestra di dialogo ***Scansione Anti-Rootkit in corso*** che indica l'avanzamento della scansione avviata:

Modifica della configurazione della scansione

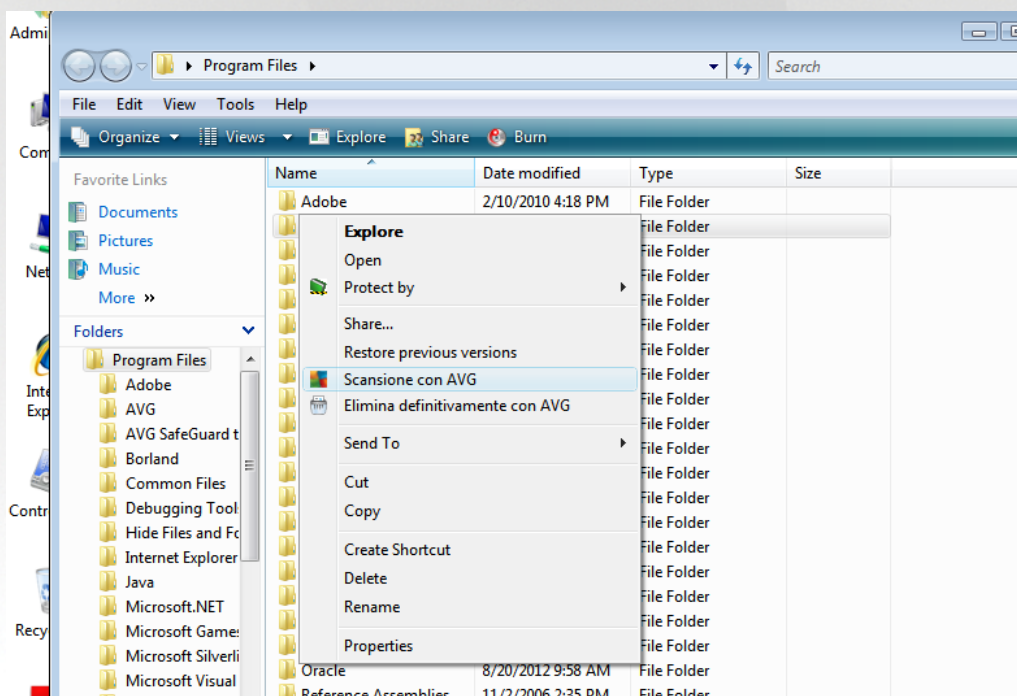
È possibile modificare la configurazione della scansione Anti-Rootkit nella finestra di dialogo ***Impostazioni di Anti-Rootkit*** *(accessibile tramite il collegamento Impostazioni per la scansione Esegui la ricerca di rootkit nel computer nella finestra di dialogo Opzioni di scansione)*. ***Si consiglia di mantenere le impostazioni predefinite e di modificarle solo se esiste un reale motivo per farlo.***

Scansione applicazioni e ***Scansione driver*** consentono di specificare in dettaglio gli elementi da includere nella scansione Anti-Rootkit. Queste impostazioni sono progettate per utenti esperti. Si consiglia di lasciare

attivate tutte le opzioni. È inoltre possibile selezionare la modalità di scansione rootkit:

- ***Scansione rapida rootkit***: sottopone a scansione tutti i processi in esecuzione, tutti i driver caricati e la cartella di sistema (*solitamente c:\Windows*)
- ***Scansione completa rootkit***: sottopone a scansione tutti i processi in esecuzione, tutti i driver caricati e la cartella di sistema (*solitamente c:\Windows*), nonché tutte le unità locali (*inclusa l'unità di memoria flash, ma escluse le unità disco floppy/CD*)

8.2. Scansione in Esplora risorse

Oltre alle scansioni predefinite avviate per l'intero computer o per le aree selezionate, **AVG AntiVirus** offre l'opzione di scansione rapida di un oggetto specifico direttamente nell'ambiente Esplora risorse. Se si desidera aprire un file sconosciuto e non si è sicuri del contenuto, è possibile decidere di eseguire un controllo su richiesta. Procedere come segue:

- In Esplora risorse evidenziare il file *o la cartella* che si desidera verificare
- Fare clic con il pulsante destro del mouse sull'oggetto per aprire il menu di scelta rapida
- Selezionare l'opzione ***Scansione con AVG*** per eseguire la scansione con **AVG AntiVirus**

8.3. Scansione dalla riga di comando

In **AVG AntiVirus** è possibile eseguire la scansione dalla riga di comando. Ad esempio, è possibile utilizzare questa opzione sui server oppure durante la creazione di uno script batch da avviare automaticamente dopo l'avvio del computer. Dalla riga di comando, è possibile avviare la scansione mentre nell'interfaccia utente grafica di AVG viene fornita la maggior parte dei parametri.

Per avviare la scansione di AVG dalla riga di comando, eseguire il seguente comando dalla cartella in cui è

stato installato AVG:

- ***avgscanx*** per sistemi operativi a 32 bit
- ***avgscana*** per sistemi operativi a 64 bit

Sintassi del comando

La sintassi del comando è la seguente:

- ***avgscanx /parametro*** ... ad esempio ***avgscanx /comp*** per la scansione dell'intero computer
- ***avgscanx /parametro /parametro*** .. nel caso di più parametri, questi dovrebbero essere allineati in una riga e separati da uno spazio e dal carattere della barra (/)
- se per un parametro è necessario fornire un valore specifico (ad esempio, il parametro ***/scan*** richiede informazioni relative alle aree del computer di cui eseguire la scansione ed è necessario fornire il percorso esatto della sezione selezionata), i valori vengono separati da punto e virgola. Ad esempio: ***avgscanx /scan=C:\;D:***

Parametri di scansione

Per visualizzare una panoramica completa dei parametri disponibili, digitare il rispettivo comando insieme al parametro /? o /HELP (ad esempio ***avgscanx /?***). Nota: l'unico parametro obbligatorio è /SCAN, che consente di specificare quali aree del computer devono essere sottoposte a scansione. Per spiegazioni più dettagliate delle opzioni, vedere la panoramica dei parametri da riga di comando.

Per eseguire la scansione, premere ***Invio***. Durante la scansione è possibile arrestare il processo premendo ***Ctrl+C*** oppure ***Ctrl+Pausa***.

Scansione CMD avviata dall'interfaccia grafica

Quando viene eseguita la modalità provvisoria di Windows, è inoltre possibile avviare la scansione da riga di comando dall'interfaccia utente grafica. La scansione verrà avviata dalla riga di comando. La finestra di dialogo ***Compositore riga di comando*** consente solo di specificare la maggior parte dei parametri di scansione nella comoda interfaccia grafica.

Poiché questa finestra di dialogo è accessibile solo nella modalità provvisoria di Windows, per ulteriori informazioni consultare il file della Guida aperto direttamente dalla finestra di dialogo.

8.3.1. Parametri scansione CMD

Di seguito viene fornito un elenco di tutti i parametri disponibili per la scansione dalla riga di comando:

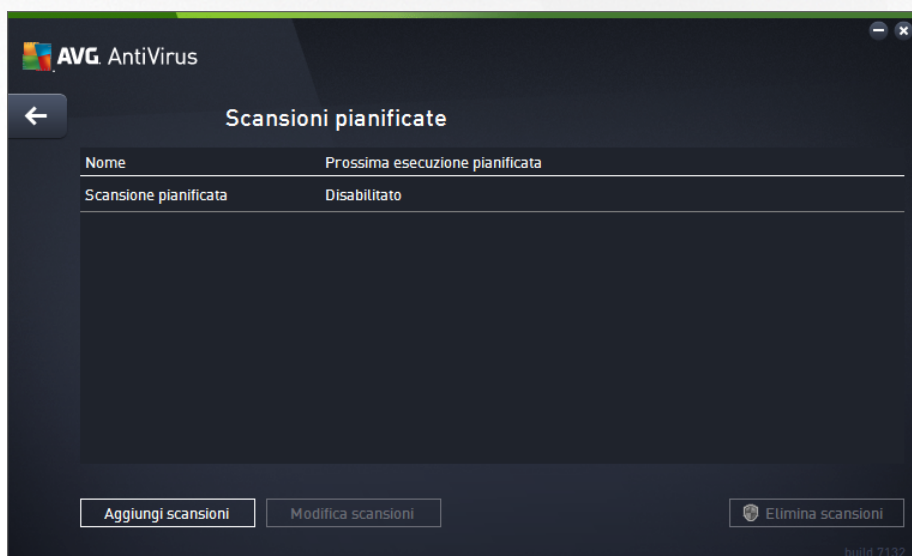
- /SCAN Scansione file o cartelle /SCAN=percorso;percorso *(ad esempio /SCAN=C:\;D:\)*
- /COMP Scansione intero computer
- /HEUR Utilizzo dell'analisi euristica

- /EXCLUDE Esclusione di un percorso o di file dalla scansione
- /@ File di comando /nome file/
- /EXT Scansione delle estensioni specificate /ad esempio EXT=EXE,DLL/
- /NOEXT Esclusione dalla scansione delle estensioni specificate /ad esempio NOEXT=JPG/
- /ARC Scansione degli archivi
- /CLEAN Pulizia automatica
- /TRASH Spostamento dei file infetti in Quarantena virus
- /QT Controllo rapido
- /LOG Generazione di un file dei risultati della scansione
- /MACROW Segnalazione delle macro
- /PWDW Segnalazione dei file protetti da password
- /ARCBOMBSW Segnalazione delle bombe a decompressione *(archivi compressi più volte)*
- /IGNLOCKED Esclusione dei file bloccati
- /REPORT Creazione di un rapporto nel file /nome file/
- /REPAPPEND Aggiunta al file di rapporto
- /REPOK Segnalazione dei file non infetti come OK
- /NOBREAK Interruzione tramite CTRL-BREAK non consentita
- /BOOT Abilitazione del controllo MBR/BOOT
- /PROC Scansione dei processi attivi
- /PUP Segnalazione delle applicazioni potenzialmente indesiderate
- /PUPEXT Segnalazione dei set potenziati di applicazioni potenzialmente indesiderate
- /REG Scansione del Registro di sistema
- /COO Scansione dei cookie
- /? Visualizzazione della Guida in linea sull'argomento
- /HELP Visualizzazione della Guida in linea sull'argomento
- /PRIORITY Impostazione della priorità per la scansione /bassa, automatica, alta/ *(vedere Impostazioni avanzate / Scansioni)*

- /SHUTDOWN Arresto del computer al completamento della scansione
- /FORCESHUTDOWN Arresto forzato del computer al completamento della scansione
- /ADS Scansione dei flussi di dati alternativi *(solo NTFS)*
- /HIDDEN Segnalazione dei file con estensione nascosta
- /INFECTABLEONLY Scansione dei soli file con estensioni infettabili
- /THOROUGHSCAN Attivazione della scansione completa
- /CLOUDCHECK Ricerca di falsi positivi
- /ARCBOMBSW Segnalazione dei file di archivio ricompressi

8.4. Pianificazione di scansioni

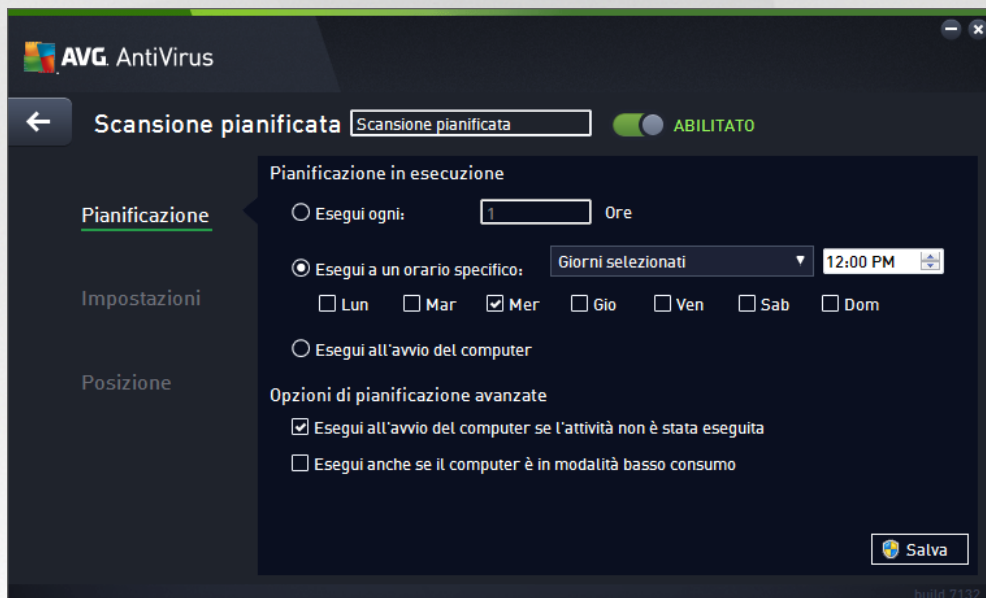
AVG AntiVirus consente di eseguire scansioni su richiesta *(ad esempio quando si sospetta che un'infezione sia stata trasferita nel computer)* oppure in base a una pianificazione. Si consiglia di eseguire le scansioni in base a una pianificazione: in questo modo ci si assicura che il computer sia protetto da possibili infezioni e non è necessario preoccuparsi dell'avvio della scansione. Scansione intero computer deve essere avviata regolarmente, almeno una volta alla settimana. Tuttavia, se possibile, avviare la scansione dell'intero computer ogni giorno, come impostato nella configurazione predefinita della pianificazione della scansione. Se il computer è sempre acceso, è possibile pianificare le scansioni fuori dagli orari di lavoro. Se il computer rimane a volte spento, è possibile pianificare l'esecuzione delle scansioni all'avvio del computer, nel caso in cui l'attività non sia stata eseguita.

La pianificazione di scansione può essere creata / modificata nella finestra di dialogo ***Scansioni pianificate*** accessibile tramite il pulsante ***Gestione scansioni pianificate*** nella finestra di dialogo Opzioni di scansione. Nella nuova finestra di dialogo ***Scansione pianificata*** è possibile visualizzare una panoramica completa di tutte le scansioni pianificate al momento:

Nella finestra di dialogo è possibile specificare le scansioni personalizzate. Utilizzare il pulsante ***Aggiungi***

scansione pianificata per creare una nuova pianificazione di scansione personalizzata. È possibile modificare i parametri della scansione pianificata (*o configurare una nuova pianificazione*) in tre schede:

- Pianificazione
- Impostazioni
- Posizione

In ogni scheda è possibile impostare il pulsante "semaforo" per disattivare temporaneamente il controllo pianificato e riattivarlo secondo le necessità.

8.4.1. Pianificazione

Nella parte superiore della scheda ***Pianificazione*** è disponibile il campo di testo in cui specificare il nome della pianificazione di scansione che si sta definendo attualmente. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro. Ad esempio, non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Tuttavia, un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via.

In questa finestra di dialogo è possibile definire ulteriormente i seguenti parametri della scansione:

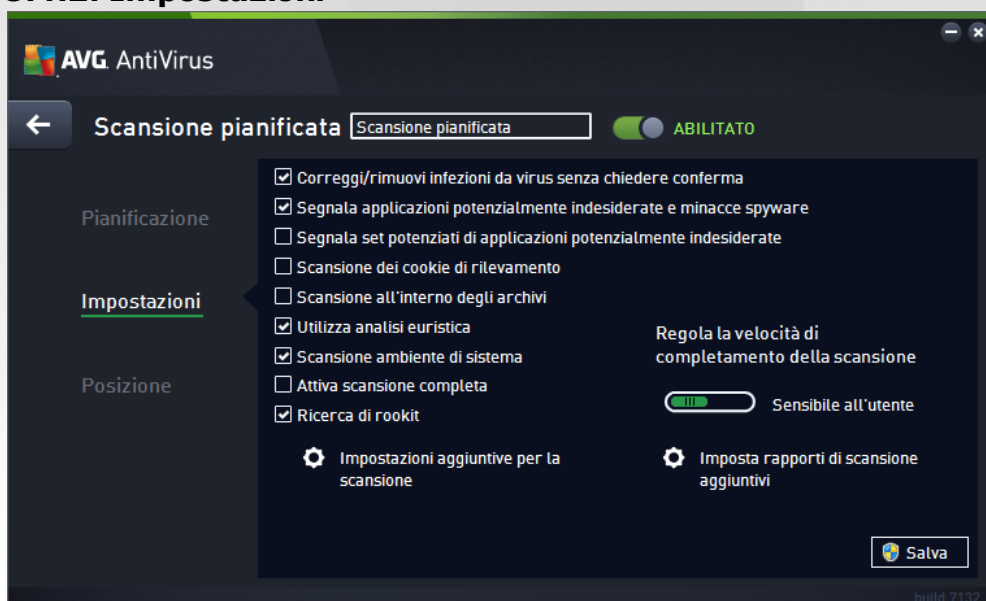
- ***Pianificazione esecuzione***: consente di specificare gli intervalli di tempo per l'avvio della nuova scansione pianificata. È possibile definire l'ora tramite l'avvio ripetuto della scansione dopo un certo periodo di tempo *(Esegui ogni...)*, specificando data e ora esatte *(Esegui a un orario specifico)*, oppure definendo un evento a cui dovrà essere associato l'avvio della scansione *(Esegui all'avvio del computer)*.

- ***Opzioni di pianificazione avanzate***: questa sezione consente di definire le circostanze in cui deve essere avviata o non avviata la scansione se il computer si trova in modalità basso consumo oppure se è completamente spento. Quando la scansione pianificata viene avviata in corrispondenza dell'ora specificata, l'utente ne viene informato tramite una finestra popup visualizzata sopra l'icona della barra

delle applicazioni di AVG. Viene quindi visualizzata una nuova icona della barra delle applicazioni di AVG (completamente colorata e con una luce lampeggiante) per comunicare che è in corso una scansione pianificata. Fare clic con il pulsante destro del mouse sull'icona AVG della scansione in esecuzione per aprire un menu di scelta rapida in cui è possibile decidere se sospendere o arrestare la scansione in esecuzione, nonché modificarne la priorità.

Controlli nella finestra di dialogo

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle scansioni pianificate. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.
- : usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle scansioni pianificate.

8.4.2. Impostazioni

Nella parte superiore della scheda ***Impostazioni*** è possibile trovare il campo di testo in cui specificare il nome della pianificazione di scansione che si sta definendo attualmente. Denominare le scansioni assegnando sempre nomi brevi, descrittivi e appropriati per poterle riconoscere più facilmente in futuro. Ad esempio, non è appropriato denominare una scansione "Nuova scansione" o "Scansione personale" poiché questi nomi non fanno riferimento agli elementi sottoposti a scansione. Un esempio di un buon nome descrittivo potrebbe essere "Scansione aree di sistema" e così via.

Nella scheda ***Impostazioni*** è contenuto un elenco di parametri di scansione che possono essere attivati/disattivati facoltativamente. ***A meno che ci sia una ragione valida per modificare le impostazioni, si consiglia di mantenere la configurazione predefinita***:

- ***Correggi/Rimuovi infezioni da virus senza richiedere conferma*** *(attivata per impostazione predefinita):* se viene identificato un virus durante la scansione può essere corretto automaticamente se è disponibile una soluzione. Se il file infetto non può essere corretto automaticamente, l'oggetto

infetto verrà spostato in Quarantena virus.

- ***Segnala applicazioni potenzialmente indesiderate e minacce spyware*** *(attivata per impostazione predefinita):* selezionare questa casella di controllo per attivare la scansione per ricercare spyware e virus. Gli spyware rappresentano una categoria di malware anomala: anche se solitamente costituiscono un rischio per la sicurezza, alcuni di questi programmi possono essere installati intenzionalmente. Si consiglia di mantenere questa funzionalità attivata in quanto consente di aumentare la protezione del computer.

- ***Segnala set potenziati di applicazioni potenzialmente indesiderate*** (*disattivata per impostazione predefinita*): selezionare per rilevare pacchetti estesi di spyware, ovvero programmi perfettamente normali e innocui al momento dell'acquisto diretto presso il produttore, ma utilizzabili a scopi dannosi successivamente. Si tratta di una precauzione aggiuntiva che aumenta ulteriormente la protezione del computer, ma che potrebbe bloccare programmi legittimi, pertanto l'opzione è disattivata per impostazione predefinita.

- ***Scansione dei cookie di rilevamento*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che i cookie devono essere rilevati durante la scansione (*i cookie HTTP vengono utilizzati per autenticare, rilevare e mantenere informazioni specifiche sugli utenti, quali i siti preferiti o il contenuto dei carrelli elettronici*).

- ***Scansione all'interno degli archivi*** (*disattivata per impostazione predefinita*): questo parametro stabilisce che la scansione deve controllare tutti i file anche se inclusi all'interno di un tipo di archivio, quale ZIP, RAR e così via.

- ***Usa analisi euristiche*** (*attivata per impostazione predefinita*): l'analisi euristica (*emulazione dinamica delle istruzioni dell'oggetto sottoposto a scansione in un ambiente informatico virtuale*) sarà uno dei metodi utilizzati per il rilevamento di virus durante la scansione.

- ***Scansione ambiente di sistema*** (*attivata per impostazione predefinita*): la scansione verrà eseguita anche sulle aree di sistema del computer.

- ***Attiva scansione completa*** (*disattivata per impostazione predefinita):* in situazioni specifiche (*ad esempio se si sospetta che il computer sia stato infettato*) per maggiore sicurezza è possibile selezionare questa opzione per attivare gli algoritmi di scansione più completi che esamineranno anche le aree del computer che difficilmente vengono infettate. Tenere presente tuttavia che questo metodo è piuttosto dispendioso in termini di tempo.

- ***Ricerca di rootkit*** *(attivata per impostazione predefinita):* la scansione Anti-Rootkit ricerca sul computer la presenza di eventuali rootkit (programmi e tecnologie in grado di coprire l'attività dei malware nel computer). Se viene rilevato un rootkit, ciò non significa necessariamente che il computer sia infetto. In alcuni casi, specifici driver o sezioni di applicazioni regolari possono venire rilevati erroneamente come rootkit.

Impostazioni di scansione aggiuntive

Il collegamento consente di aprire una nuova finestra di dialogo ***Impostazioni di scansione aggiuntive*** in cui è possibile specificare i seguenti parametri:

- ***Opzioni arresto computer***: consente di decidere se il computer deve essere arrestato automaticamente al termine del processo di scansione. Dopo aver confermato questa opzione *(Arresta computer al completamento della scansione)*, viene attivata una nuova opzione che consente l'arresto del computer anche se è correntemente bloccato *(Forza arresto se il computer è bloccato)*.

- ***Tipi di file per la scansione***: specificare se si desidera sottoporre a scansione:

  - ***Tutti i tipi di file*** con l'opzione per definire le eccezioni fornendo un elenco di estensioni di file separate da virgola da non sottoporre a scansione.

  - ***Tipi di file selezionati***: è possibile specificare che si desidera sottoporre a scansione solo i file potenzialmente infettabili *(i file che non possono essere infettati non verranno sottoposti a scansione, ad esempio alcuni file di testo normale o altri file non eseguibili)*, inclusi i file multimediali *(file video e audio; se non si seleziona questa casella, il tempo di scansione risulterà ulteriormente ridotto, poiché questi file sono spesso di grandi dimensioni e non facilmente infettabili da un virus)*. Anche in questo caso, è possibile specificare tramite le estensioni quali file devono essere sempre sottoposti a scansione.

  - Facoltativamente, è possibile effettuare la ***Scansione dei file senza estensioni***: questa opzione è attivata per impostazione predefinita e si consiglia di non modificarla a meno che non si abbiano motivi validi per farlo. I file senza estensione sono piuttosto sospetti e devono essere sempre sottoposti a scansione.

Regola la velocità di completamento della scansione

All'interno di questa sezione è inoltre possibile specificare la velocità di scansione desiderata in base all'utilizzo delle risorse di sistema. Per impostazione predefinita, questa opzione è impostata sul livello *Sensibile all'utente* per l'utilizzo automatico delle risorse. Se si desidera aumentare la velocità della scansione, il tempo impiegato sarà inferiore ma l'utilizzo delle risorse di sistema aumenterà notevolmente durante l'esecuzione e rallenterà le altre attività svolte sul PC (*questa opzione può essere utilizzata quando il computer è acceso ma non in uso*). Tuttavia, è possibile diminuire l'utilizzo delle risorse di sistema aumentando la durata della scansione.

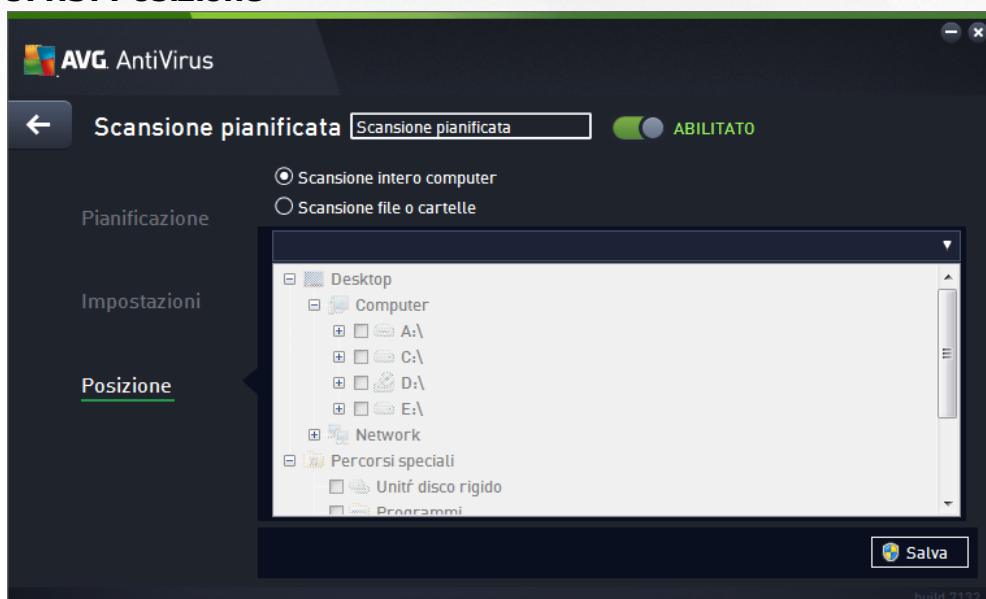
Imposta rapporti di scansione aggiuntivi

Fare clic sul collegamento ***Imposta rapporti di scansione aggiuntivi...*** per aprire una finestra di dialogo autonoma denominata ***Rapporti di scansione*** in cui è possibile selezionare diversi elementi per definire i tipi di rilevamenti da segnalare:

Controlli nella finestra di dialogo

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle scansioni pianificate. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- : usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle scansioni pianificate.

8.4.3. Posizione

Nella scheda ***Posizione*** è possibile definire se si desidera pianificare la scansione dell'intero computer o la scansione di file o cartelle. Se si seleziona la scansione di cartelle o file, nella parte inferiore di questa finestra di dialogo viene attivata la struttura visualizzata che consente di specificare le cartelle da sottoporre a scansione (*espandere le voci facendo clic sul nodo "+" finché non viene individuata la cartella da sottoporre a scansione*). È possibile selezionare più cartelle facendo clic sulle rispettive caselle. Le cartelle selezionate verranno visualizzate nel campo di testo nella parte superiore della finestra di dialogo e nel menu a discesa verrà mantenuta la cronologia delle scansioni selezionate per riferimento futuro. In alternativa, è possibile immettere manualmente il percorso completo della cartella desiderata (*se si immettono più percorsi, è necessario separarli con un punto e virgola senza ulteriori spazi*).

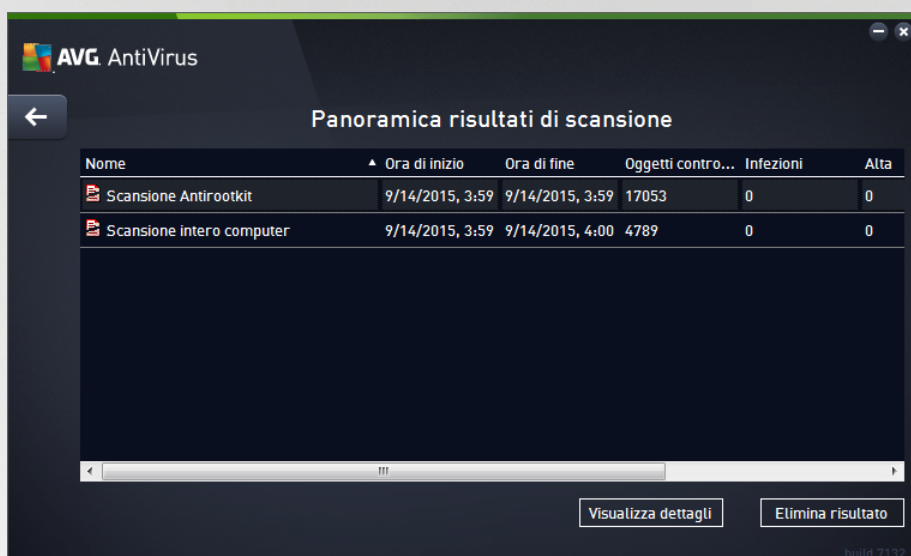
All'interno della struttura è inoltre possibile visualizzare un ramo denominato ***Percorsi speciali***. Di seguito è disponibile un elenco delle posizioni che verranno sottoposte a scansione se verrà selezionata la relativa casella di controllo:

- ***Dischi rigidi locali***: tutti i dischi rigidi del computer
- ***Programmi***
  - C:\Programmi\
  - *nella versione a 64 bit* C:\Programmi (x86)
- ***Cartella Documenti***
  - *per Windows XP:* C:\Documents and Settings\utente predefinito\Documenti\
  - *per Windows Vista/7*: C:\Users\utente\Documenti\
- ***Documenti condivisi***
  - *per Windows XP*: C:\Documents and Settings\All Users\Documenti condivisi\
  - *per Windows Vista/7*: C:\Users\Public\Documenti condivisi\
- ***Cartella Windows***: C:\Windows\
- ***Altro***
  - *Unità di sistema*: disco rigido su cui è installato il sistema operativo (solitamente C:)
  - *Cartella di sistema*: C:\Windows\System32\
  - *Cartella file temporanei*: C:\Documents and Settings\utente\Local\ (*Windows XP*) oppure C:\Users\utente\AppData\Local\Temp\ (*Windows Vista/7*)
  - *File temporanei di Internet*: C:\Documents and Settings\utente\Local Settings\Temporary Internet Files\ (*Windows XP*); oppure C:\Users\utente\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Controlli nella finestra di dialogo

- ***Salva***: consente di salvare tutte le modifiche eseguite su questa scheda o su un'altra scheda della finestra di dialogo e di tornare alla panoramica delle scansioni pianificate. Pertanto, se si desidera configurare i parametri di controllo di tutte le schede, selezionare il pulsante per salvarli solo dopo aver specificato tutti i requisiti desiderati.

- : usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare alla panoramica delle scansioni pianificate.

8.5. Risultati scansione

Nella finestra di dialogo ***Panoramica risultati di scansione*** è contenuto l'elenco dei risultati di tutte le scansioni eseguite in precedenza. Il grafico fornisce le seguenti informazioni su ciascun risultato della scansione:

- ***Icona***: nella prima colonna è visualizzata un'icona informativa che descrive lo stato della scansione:
  - Nessuna infezione rilevata, scansione completata
  - Nessuna infezione rilevata, scansione interrotta prima del completamento
  - Infezioni rilevate e non corrette, scansione completata
  - Infezioni rilevate e non corrette, scansione interrotta prima del completamento
  - Infezioni rilevate e corrette o rimosse, scansione completata
  - Infezioni rilevate e corrette o rimosse, scansione interrotta prima del completamento

- ***Nome***: in questa colonna viene visualizzato il nome della rispettiva scansione. Si tratta di una delle due scansioni predefinite oppure della scansione pianificata dall'utente.

- ***Ora di inizio***: indica la data e l'ora esatte di avvio della scansione.

- ***Ora di fine***: indica la data e l'ora esatte in cui la scansione è stata completata, sospesa o interrotta.
- ***Oggetti controllati***: indica il numero totale di tutti gli oggetti sottoposti a scansioni.
- ***Infezioni***: indica il numero di infezioni rilevate totali/rimosse.
- ***Alto / Medio / Basso***: le seguenti colonne indicano il numero di infezioni rilevate con livello di gravità alto, medio o basso rispettivamente.
- ***Rootkit***: indica il numero totale di rootkit rilevati durante la scansione.

Comandi della finestra di dialogo

Visualizza dettagli: fare clic sul pulsante per visualizzare informazioni dettagliate su una scansione selezionata *(evidenziata nel grafico sopra)*.

Elimina risultati: fare clic sul pulsante per rimuovere un risultato della scansione selezionato nel grafico.

: usare la freccia verde nella parte superiore sinistra della finestra di dialogo per tornare all'interfaccia utente principale con la panoramica dei componenti.

8.6. Dettagli di Risultati scansione

Per aprire una panoramica delle informazioni dettagliate su un risultato scansione selezionato, fare clic sul pulsante ***Visualizza dettagli*** disponibile nella finestra di dialogo Panoramica risultati di scansione. Si verrà reindirizzati alla stessa interfaccia che descrive dettagliatamente le informazioni sui rispettivi risultati della scansione. Le informazioni sono divise in tre schede:

- ***Riepilogo***: questa scheda fornisce informazioni di base sulla scansione (se è stata completata, se sono state rilevate minacce e l'operazione che è stata eseguita su di esse).
- ***Dettagli***: in questa scheda vengono visualizzate tutte le informazioni sulla scansione, inclusi i dettagli relativi a eventuali minacce rilevate. Esporta panoramica nel file consente di salvarla come file .csv.
- ***Rilevamenti***: questa scheda viene visualizzata solo se sono state rilevate minacce durante la scansione e fornisce informazioni dettagliate sulle minacce.

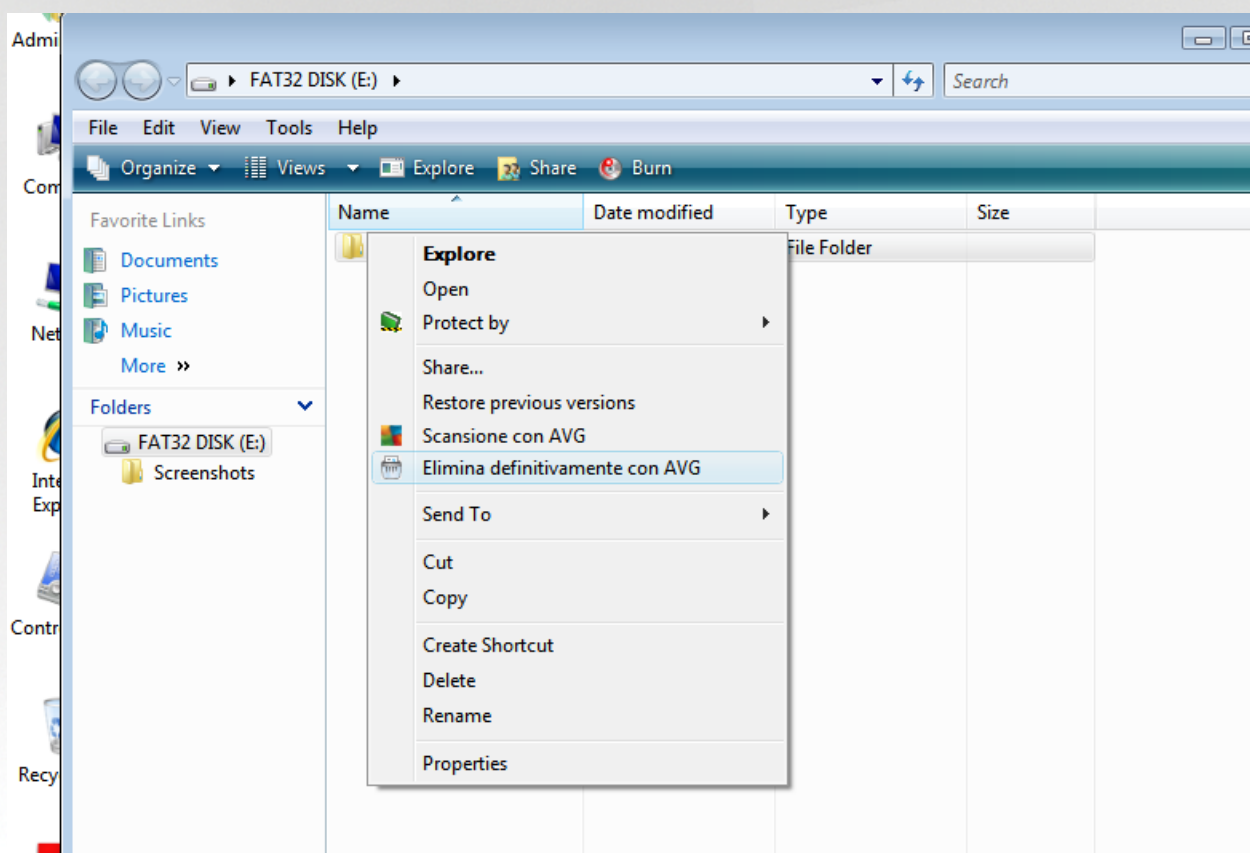
  Livello di gravità informazioni: informazioni o avvisi, non minacce effettive. In genere, documenti che contengono macro, documenti o archivi protetti da password, file bloccati e così via.

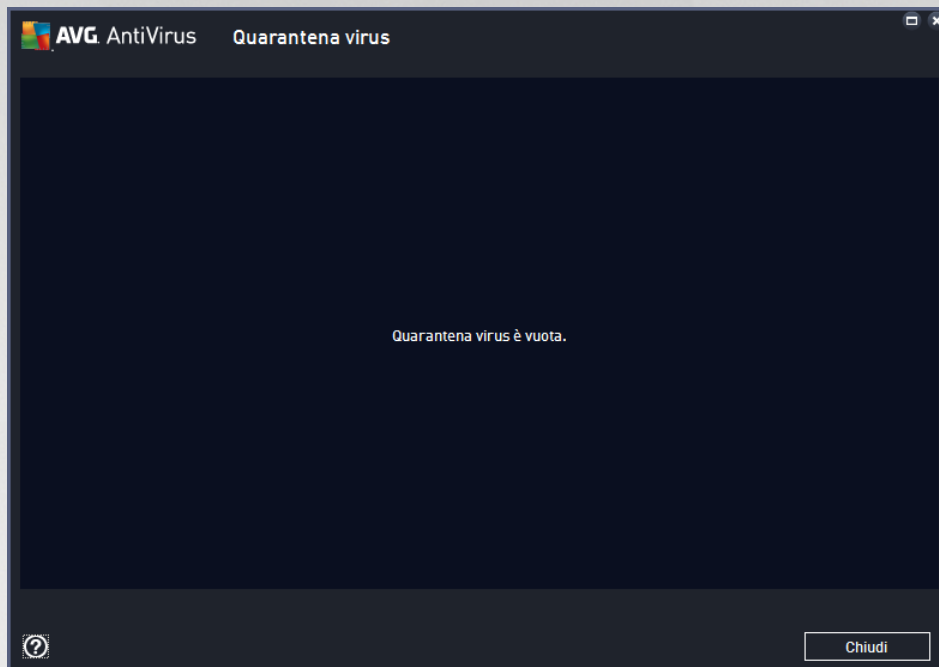
  Livello di gravità medio: PUP (programmi potenzialmente indesiderati, *come ad esempio adware)* o cookie di rilevamento

  Livello di gravità alto: minacce gravi come virus, trojan, exploit e così via. Anche oggetti individuati dal metodo di rilevamento dell'analisi euristica, ovvero minacce non ancora descritte nel database dei virus.

9. AVG File Shredder

AVG File Shredder è stato creato per eliminare i file in tutta sicurezza, ovvero senza possibilità di ripristinarli, neppure con strumenti software avanzati specifici per questo scopo.

Per eliminare definitivamente un file o una cartella, fare clic con il pulsante destro del mouse su un file manager *(Esplora risorse, Total Commander e così via)* e selezionare ***Elimina definitivamente con AVG*** dal menu di scelta rapida. Anche i file presenti nel Cestino possono essere eliminati definitivamente. Se non è possibile eliminare in modo definitivo e affidabile un file specifico in un percorso specifico *(ad esempio, in un CD-ROM)*, verrà visualizzata una notifica o l'opzione nel menu di scelta rapida non sarà disponibile.

È importante tenere presente che dopo aver eliminato un file in modo definitivo, non sarà possibile recuperarlo.

10. Quarantena virus

Quarantena virus è un ambiente protetto per la gestione degli oggetti sospetti o infetti rilevati durante i controlli AVG. Se durante la scansione viene rilevato un oggetto infetto e AVG non è in grado di ripararlo automaticamente, viene richiesto quale operazione eseguire sull'oggetto sospetto. La soluzione consigliata è spostare l'oggetto in ***Quarantena virus*** per un'ulteriore elaborazione. Lo scopo principale di ***Quarantena virus*** è quello di conservare ciascun file eliminato per un periodo di tempo sufficiente ad accertare che il file non sia più necessario nella posizione originale. Se l'assenza del file dovesse causare problemi, è possibile inviare il file in questione per l'analisi o ripristinarlo nella posizione originale.

L'interfaccia di ***Quarantena virus*** viene aperta in una finestra separata e offre una panoramica delle informazioni relative agli oggetti infetti messi in quarantena:

- ***Data aggiunta***: data e ora del rilevamento e dell'inserimento in Quarantena virus del file sospetto.
- ***Minaccia***: se è stato installato il componente Identity in **AVG AntiVirus**, questa sezione fornirà l'identificazione grafica della gravità del rilevamento: dal livello più sicuro *(tre punti verdi)* al più pericoloso *(tre punti rossi)*. Saranno inoltre disponibili informazioni sul tipo di infezione e sulla posizione originale. Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'enciclopedia dei virus online.
- ***Origine***: specifica il componente di **AVG AntiVirus** da cui è stata rilevata la rispettiva minaccia.
- ***Notifiche***: in alcune situazioni, in questa colonna possono essere visualizzate note con commenti dettagliati sulla rispettiva minaccia rilevata.

Pulsanti di controllo

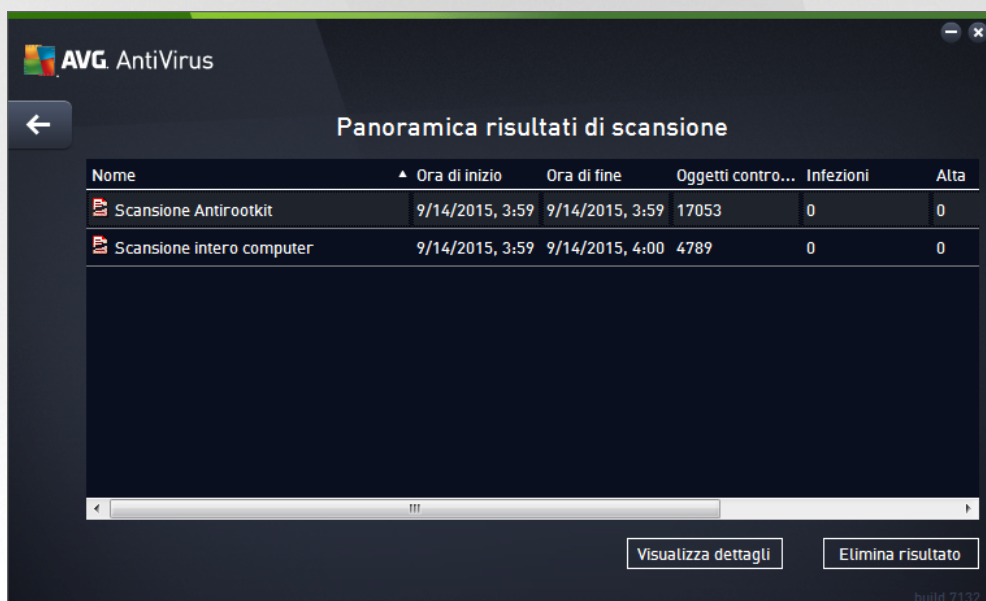
I seguenti pulsanti di controllo sono accessibili dall'interfaccia di ***Quarantena virus***:

- ***Ripristina***: consente di ripristinare il file infetto nella posizione originale sul disco.
- ***Ripristina come***: sposta il file infetto nella cartella selezionata.
- ***Invia per analisi***: il pulsante è attivo solo quando si evidenzia un oggetto nell'elenco dei rilevamenti superiore. In tal caso, è possibile inviare il rilevamento selezionato ai Virus Lab di AVG per un'ulteriore analisi dettagliata. Tenere presente che questa funzionalità deve essere utilizzata principalmente per inviare i falsi positivi, ovvero i file rilevati da AVG come infetti o sospetti, ma ritenuti innocui dall'utente.
- ***Dettagli***: per informazioni dettagliate sulla minaccia specifica spostata in ***Quarantena virus*** evidenziare l'elemento selezionato nell'elenco e fare clic sul pulsante ***Dettagli*** per aprire una nuova finestra di dialogo con la descrizione della minaccia rilevata.
- ***Elimina***: consente di rimuovere definitivamente il file infetto da ***Quarantena virus***.
- ***Svuota Quarantena***: elimina completamente tutto il contenuto di ***Quarantena Virus***. I file rimossi da ***Quarantena virus*** vengono eliminati in modo definitivo dal disco (*non vengono spostati nel Cestino*).

11. Cronologia

La sezione ***Cronologia*** include informazioni su tutti gli eventi precedenti *(ad esempio aggiornamenti, scansioni, rilevamenti e così via)* e i rapporti relativi a tali eventi. Questa sezione è accessibile dall'interfaccia utente principale tramite la voce ***Opzioni / Cronologia***. Inoltre, la cronologia di tutti gli eventi registrati è suddivisa nelle seguenti parti:

- Risultati scansione
- Risultati di Resident Shield
- Risultati di Protezione email
- Risultati di Online Shield
- Cronologia eventi

11.1. Risultati scansione

La finestra di dialogo ***Panoramica risultati di scansione*** è accessibile tramite la voce ***Opzioni / Cronologia / Risultati scansione*** nel menu di spostamento superiore della finestra principale di **AVG AntiVirus**. Nella finestra di dialogo è contenuto l'elenco di tutte le scansioni avviate in precedenza e le informazioni sui relativi risultati:

- ***Nome***: nome della scansione; può essere il nome di una delle scansioni predefinite o il nome assegnato alla propria scansione pianificata. Ciascun nome include un'icona che indica i risultati della scansione:

  – il colore verde indica che non è stata rilevata alcuna infezione durante la scansione

  – il colore blu indica che è stata rilevata un'infezione durante la scansione ma l'oggetto infetto è stato rimosso automaticamente

– il colore rosso indica che è stata rilevata un'infezione durante la scansione ma non è stato possibile rimuoverla.

Ciascuna icona può essere intera o suddivisa in due parti: l'icona intera indica una scansione completata correttamente, l'icona suddivisa in due indica una scansione annullata o interrotta.

***Nota**: per informazioni dettagliate su ciascuna icona vedere la finestra di dialogo Risultati scansione accessibile tramite il pulsante Visualizza dettagli (nella parte inferiore della finestra di dialogo).*

- ***Ora di inizio***: data e ora di avvio della scansione
- ***Ora di fine***: data e ora del completamento della scansione
- ***Oggetti controllati***: numero di oggetti controllati durante la scansione
- ***Infezioni***: numero delle infezioni da virus rilevate / rimosse
- ***Alto / Medio***: queste colonne indicano il numero di infezioni totali o rimosse con livello di gravità alto o medio rispettivamente
- ***Informazioni***: informazioni relative all'andamento e al risultato della scansione *(in genere in relazione alla finalizzazione o all'interruzione)*
- ***Rootkit***: numero di rootkit

Pulsanti di controllo

I pulsanti di controllo per la finestra di dialogo ***Panoramica risultati di scansione*** sono i seguenti:

- ***Visualizza dettagli***: selezionare questa opzione per accedere alla finestra di dialogo Risultati scansione e visualizzare dati dettagliati relativi alla scansione selezionata
- ***Elimina risultato***: selezionare questa opzione per rimuovere la voce selezionata dalla panoramica dei risultati di scansione
- : per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

11.2. Risultati di Resident Shield

Il servizio ***Resident Shield*** fa parte del componente ***Computer*** ed esegue la scansione dei file mentre vengono copiati, aperti o salvati. Quando viene rilevato un virus o altra minaccia, l'utente viene avvisato immediatamente tramite la successiva finestra di dialogo:

In questa finestra di dialogo di avviso sono disponibili informazioni sull'oggetto rilevato e giudicato infetto (*Minaccia*) e alcuni dati descrittivi sull'infezione riconosciuta (*Descrizione*). Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'enciclopedia dei virus online (se note). Nella finestra di dialogo verrà inoltre visualizzata una panoramica delle soluzioni disponibili per gestire la minaccia rilevata. Una delle alternative verrà contrassegnata come consigliata: ***Proteggimi (scelta consigliata). Se possibile, si consiglia di attenersi sempre a questa opzione.***

Nota: *potrebbe accadere che le dimensioni dell'oggetto rilevato superino il limite di spazio libero in Quarantena virus. In tal caso, verrà visualizzato un avviso relativo al problema quando si tenterà di spostare l'oggetto infetto in Quarantena virus. Tuttavia, le dimensioni di Quarantena virus possono essere modificate. Tali dimensioni vengono definite come percentuale regolabile delle dimensioni effettive del disco rigido. Per aumentare le dimensioni di Quarantena virus, nella finestra di dialogo Quarantena virus, accessibile tramite Impostazioni AVG avanzate, è disponibile l'opzione Limite dimensione per Quarantena virus.*

Nella parte inferiore della finestra di dialogo è possibile trovare il collegamento ***Mostra dettagli***. Fare clic sul pulsante per aprire una nuova finestra con informazioni dettagliate sul processo in esecuzione durante il rilevamento dell'infezione e i dati identificativi del processo.

Un elenco di tutti i rilevamenti di Resident Shield è disponibile per una panoramica all'interno della finestra di dialogo ***Rilevamento Resident Shield***. Questa finestra di dialogo è accessibile tramite la voce ***Opzioni / Cronologia / Rilevamento Resident Shield*** nel menu di spostamento superiore della finestra principale di **AVG AntiVirus**. Nella finestra di dialogo è disponibile una panoramica di oggetti rilevati da Resident Shield, classificati come pericolosi e corretti o spostati in Quarantena virus.

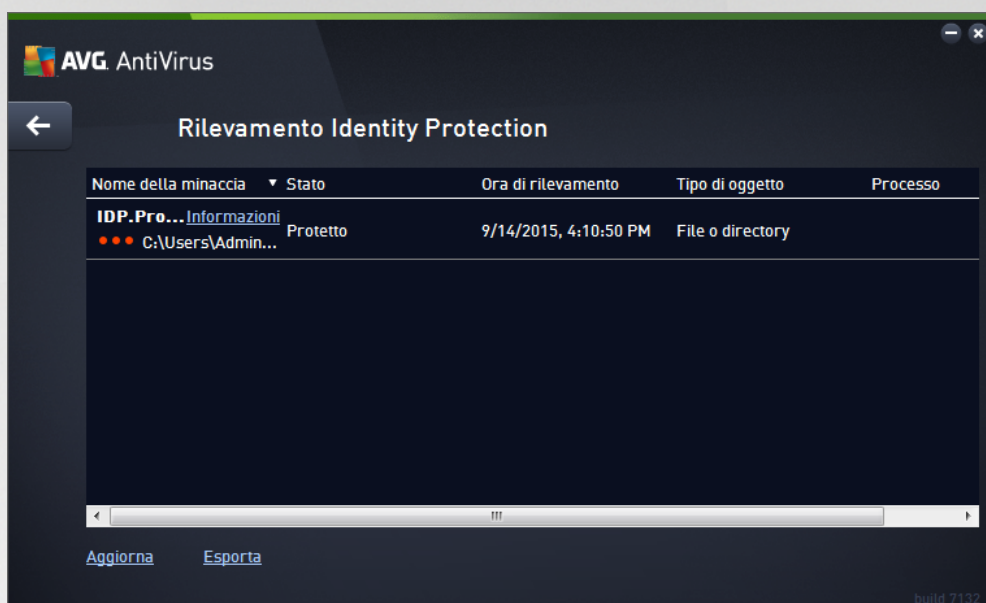
Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Nome della minaccia***: descrizione (*possibilmente anche il nome*) dell'oggetto rilevato e relativa posizione. Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'enciclopedia dei virus online.
- ***Stato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Pulsanti di controllo

- ***Aggiorna***: consente di aggiornare l'elenco dei rilevamenti effettuati da ***Online Shield***
- ***Esporta***: consente di esportare l'intero elenco di oggetti rilevati in un file
- ***Rimuovi voci selezionate***: nell'elenco è possibile evidenziare i record selezionati e utilizzare questo pulsante per eliminare solo tali elementi
- ***Rimuovi tutte le minacce***: fare clic su questo pulsante per eliminare tutti i record elencati in questa finestra di dialogo
- ←: per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

11.3. Risultati di Identity Protection

La finestra di dialogo ***Risultati di Identity Protection*** è accessibile tramite la voce ***Opzioni/ Cronologia / Risultati Identity di Protection*** nel menu di spostamento superiore della finestra principale di **AVG AntiVirus**.

La finestra di dialogo fornisce un elenco di tutti i rilevamenti effettuati dal componente Identity Protection. Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Nome della minaccia***: descrizione *(possibilmente anche il nome)* dell'oggetto rilevato e relativa posizione. Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'enciclopedia dei virus online.
- ***Stato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati sopra. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***).

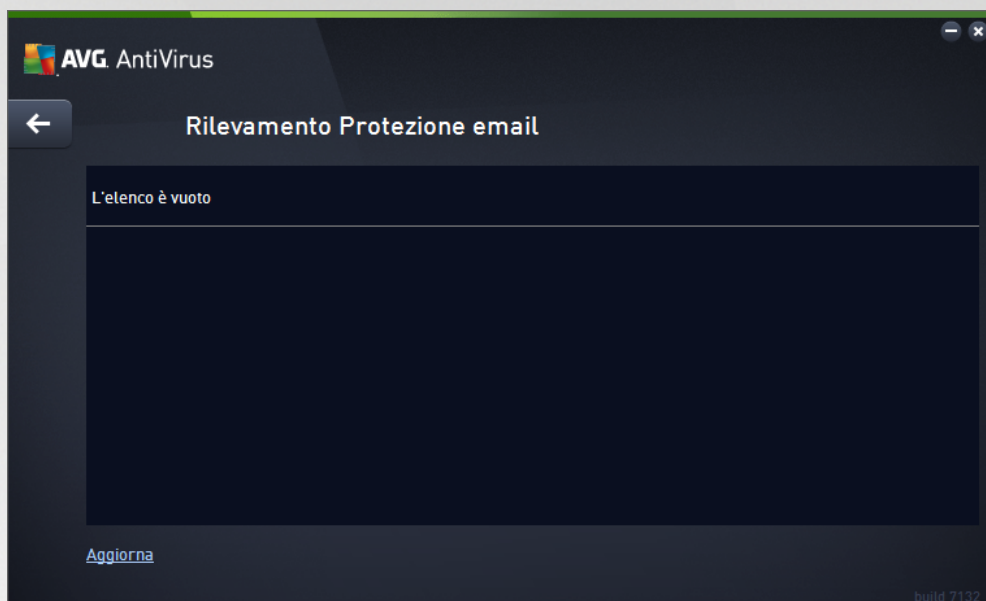
Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia ***Risultati di Identity Protection*** sono i seguenti:

- ***Aggiorna elenco***: consente di aggiornare l'elenco delle minacce rilevate
- ←: per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),*

utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

11.4. Risultati di Protezione email

La finestra di dialogo ***Risultati di Protezione email*** è accessibile tramite la voce ***Opzioni/ Cronologia / Risultati di Protezione email*** nel menu di spostamento superiore della finestra principale di **AVG AntiVirus**.

La finestra di dialogo fornisce un elenco di tutti i rilevamenti effettuati dal componente Scansione Email. Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Nome rilevamento***: descrizione *(possibilmente anche il nome)* dell'oggetto rilevato e la relativa posizione
- ***Risultato***: azione eseguita sull'oggetto rilevato
- ***Ora di rilevamento***: data e ora in cui l'oggetto sospetto è stato rilevato
- ***Tipo di oggetto***: tipo di oggetto rilevato
- ***Processo***: operazione eseguita per richiamare e rilevare l'oggetto potenzialmente pericoloso

Nella parte inferiore della finestra di dialogo, sotto l'elenco, sono disponibili informazioni sul numero totale degli oggetti rilevati elencati sopra. È inoltre possibile esportare l'intero elenco di oggetti rilevati in un file (***Esporta elenco in file***) ed eliminare tutte le voci relative agli oggetti rilevati (***Svuota elenco***).

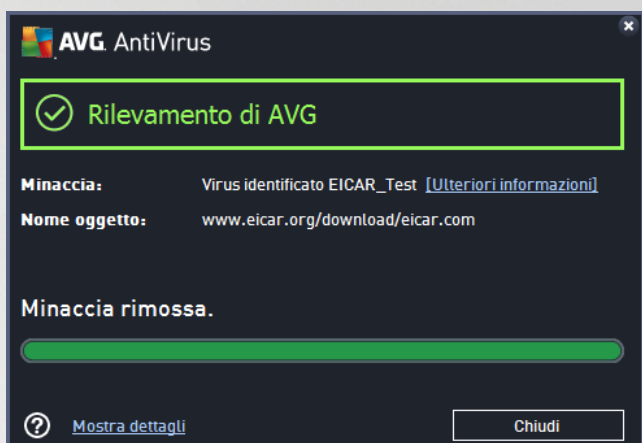
Pulsanti di controllo

I pulsanti di controllo disponibili nell'interfaccia di ***Rilevamento Scansione Email*** sono i seguenti:

- ***Aggiorna elenco***: aggiorna l'elenco delle minacce rilevate
- ←: per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),*

utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

11.5. Risultati di Online Shield

Online Shield esegue la scansione del contenuto delle pagine Web visitate e dei possibili file in esse contenuti prima che queste vengano visualizzate nel browser Web o scaricate nel computer. Se viene rilevata una minaccia, l'utente verrà avvisato immediatamente tramite la seguente finestra di dialogo:

In questa finestra di dialogo di avviso sono disponibili informazioni sull'oggetto rilevato e giudicato infetto (*Minaccia*) e alcuni dati descrittivi sull'infezione riconosciuta (*Nome oggetto*). Selezionando il collegamento *Ulteriori informazioni* si verrà reindirizzati all'enciclopedia dei virus online in cui è possibile trovare informazioni dettagliate sull'infezione rilevata (se note). La finestra di dialogo fornisce i seguenti elementi di controllo:

- ***Mostra dettagli***: fare clic sul collegamento per aprire una nuova finestra popup con informazioni sul processo in esecuzione durante il rilevamento dell'infezione e i dati identificativi del processo.
- ***Chiudi***: fare clic sul pulsante per chiudere la finestra di dialogo di avviso.

La pagina Web sospetta non verrà aperta e il rilevamento della minaccia verrà registrato nell'elenco ***Rilevamenti di Online Shield***. Questa panoramica di minacce rilevate è accessibile tramite la voce ***Opzioni / Cronologia / Rilevamenti di Online Shield*** nel menu di spostamento superiore della finestra principale di **AVG AntiVirus**.

Per ogni oggetto rilevato vengono fornite le seguenti informazioni:

- ***Nome della minaccia***: descrizione (*possibilmente anche il nome*) dell'oggetto rilevato e relativa origine (*pagina Web*). Il collegamento *Ulteriori informazioni* visualizza una pagina con informazioni dettagliate sulla minaccia rilevata, tratte dall'enciclopedia dei virus online.

- ***Stato***: azione eseguita sull'oggetto rilevato

- ***Ora di rilevamento***: data e ora in cui la minaccia è stata rilevata e bloccata

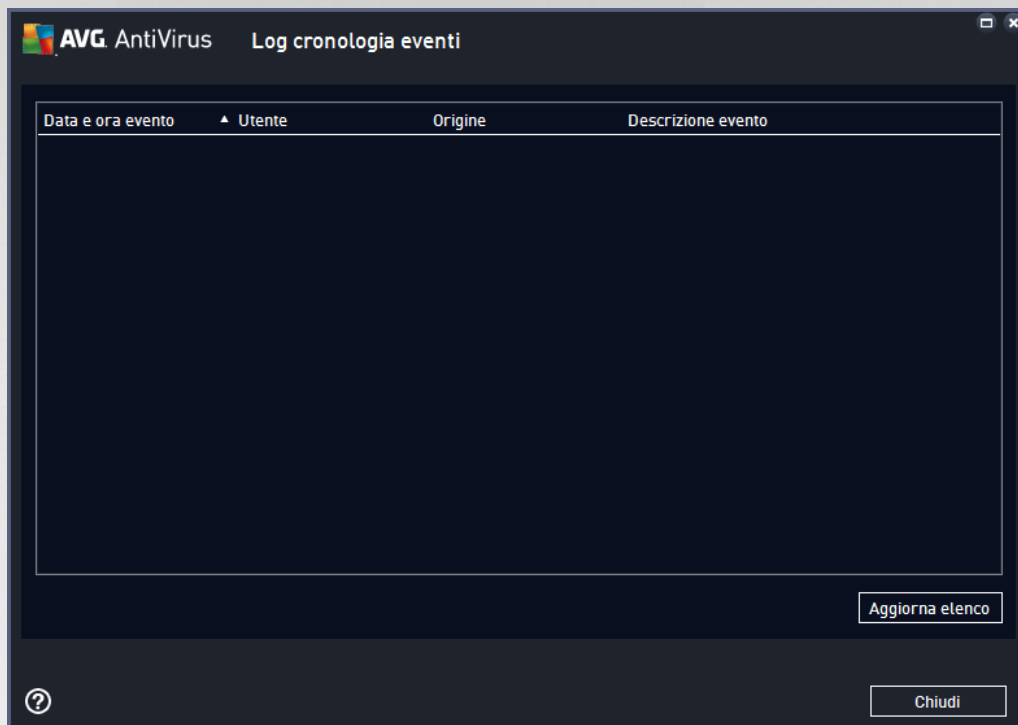
- ***Tipo di oggetto***: tipo di oggetto rilevato

Pulsanti di controllo

- ***Aggiorna***: consente di aggiornare l'elenco dei rilevamenti effettuati da ***Online Shield***

- ***Esporta***: consente di esportare l'intero elenco di oggetti rilevati in un file

- : per tornare alla finestra di dialogo principale di AVG *predefinita (panoramica dei componenti),* utilizzare la freccia nell'angolo superiore sinistro di questa finestra di dialogo

11.6. Cronologia eventi

La finestra di dialogo ***Cronologia eventi*** è accessibile tramite la voce ***Opzioni / Cronologia / Cronologia eventi*** nel menu di spostamento superiore della finestra principale di **AVG AntiVirus**. In questa finestra di dialogo è possibile trovare un riepilogo di importanti eventi che si sono verificati durante l'attività di **AVG AntiVirus**. La finestra di dialogo fornisce i record dei seguenti tipi di eventi: informazioni sugli aggiornamenti dell'applicazione AVG, informazioni sull'inizio, la fine o l'arresto della scansione (*inclusi i controlli eseguiti automaticamente*), informazioni sugli eventi connessi al rilevamento di un virus (*tramite la protezione permanente o la scansione*) inclusa la relativa posizione e altri eventi importanti.

Per ciascun evento vengono indicate le seguenti informazioni:

- ***Data e ora evento*** indica la data e l'ora esatte in cui si è verificato l'evento.
- ***Utente*** indica il nome dell'utente connesso nel momento in cui si è verificato l'evento.
- ***Origine*** fornisce informazioni sul componente di origine o altra parte del sistema AVG che ha attivato l'evento.
- ***Descrizione evento*** presenta un breve riepilogo dell'evento che si è verificato.

Pulsanti di controllo

- ***Aggiorna elenco***: fare clic su questo pulsante per aggiornare tutte le voci incluse nell'elenco degli eventi
- ***Chiudi***: fare clic sul pulsante per tornare alla finestra principale di **AVG AntiVirus**

12. Aggiornamenti di AVG

Nessun software di protezione è in grado di garantire una vera protezione dai vari tipi di minacce se non viene aggiornato con regolarità. Gli autori dei virus ricercano di continuo nuove imperfezioni da sfruttare sia nei sistemi operativi che nel software. Tutti i giorni si presentano nuovi virus, nuovi malware e nuovi attacchi di hacker. Per questa ragione, i fornitori di software rilasciano regolarmente aggiornamenti e patch di protezione per correggere eventuali difetti della protezione che vengono rilevati.

Considerando le nuove minacce informatiche emergenti e la velocità con cui si diffondono, è assolutamente fondamentale aggiornare **AVG AntiVirus** regolarmente. La soluzione migliore è attenersi alle impostazioni predefinite del programma in cui è stato configurato l'aggiornamento automatico. Tenere presente che, se il database dei virus di **AVG AntiVirus** non è aggiornato, il programma non sarà in grado di rilevare le minacce più recenti.

È fondamentale aggiornare AVG con regolarità. Gli aggiornamenti delle definizione dei virus principali dovrebbero essere eseguiti ogni giorno, se possibile. Gli aggiornamenti del programma meno urgenti possono essere eseguiti settimanalmente.

12.1. Avvio degli aggiornamenti

Per fornire la protezione massima, **AVG AntiVirus** per impostazione predefinita ricerca nuovi aggiornamenti del database dei virus ogni quattro ore. Poiché gli aggiornamenti AVG non vengono rilasciati in base a una pianificazione fissa, ma in base alla quantità e alla gravità di nuove minacce, questo check-up è molto importante per assicurare che il database dei virus di AVG sia sempre aggiornato.

Per controllare la presenza di nuovi file di aggiornamento immediatamente, utilizzare il collegamento rapido Aggiorna adesso nell'interfaccia utente principale. Questo collegamento è sempre disponibile da qualsiasi finestra di dialogo dell'interfaccia utente. Una volta avviato l'aggiornamento, AVG verificherà innanzitutto se sono presenti nuovi file di aggiornamento. In caso affermativo, **AVG AntiVirus** ne effettuerà il download e avvierà il processo di aggiornamento automaticamente. L'utente verrà informato dei risultati dell'aggiornamento nella finestra di dialogo visualizzata sopra l'icona di AVG presente nella barra delle applicazioni.

Se si desiderasse ridurre il numero di aggiornamenti avviati, è possibile impostare parametri di avvio degli aggiornamenti personalizzati. Tuttavia, ***si consiglia di avviare l'aggiornamento almeno una volta al giorno.*** La configurazione può essere modificata nella sezione Impostazioni avanzate/Pianificazioni, in particolare nelle seguenti finestre di dialogo:

- Pianificazione aggiornamento definizioni
- Pianificazione aggiornamento del programma

12.2. Livelli di aggiornamento

AVG AntiVirus offre due livelli di aggiornamento selezionabili:

- ***Aggiornamento definizioni*** contiene le modifiche necessarie per una protezione antivirus affidabile. In genere, non sono incluse eventuali modifiche del codice e viene aggiornato solo il database delle definizioni. Questo aggiornamento deve essere applicato non appena si rende disponibile.
- ***In Aggiornamento programma*** sono presenti le modifiche, le correzioni e i miglioramenti del programma.

Nel corso della pianificazione di un aggiornamento, è possibile definire parametri specifici per entrambi i livelli di aggiornamento:

- Pianificazione aggiornamento definizioni
- Pianificazione aggiornamento del programma

Nota: *se gli orari di un aggiornamento del programma pianificato e di una scansione pianificata dovessero coincidere, il processo di aggiornamento acquista priorità e la scansione viene interrotta. In questo caso l'utente verrà informato del conflitto.*

13. Domande frequenti e assistenza tecnica

Se si verificano problemi di tipo commerciale o tecnico con l'applicazione **AVG AntiVirus**, sono disponibili diversi modi per richiedere assistenza. Effettuare la scelta tra le seguenti opzioni:

- ***Ottieni assistenza***: direttamente dall'applicazione AVG è possibile visualizzare una pagina dedicata dell'assistenza clienti sul sito Web di AVG (*http://www.avg.com/*). Selezionare la voce del menu principale ***Guida / Ottieni assistenza*** per essere reindirizzati a una pagina del sito Web di AVG con le opzioni di assistenza disponibili. Per procedere, seguire le istruzioni fornite nella pagina Web.

- ***Assistenza*** *(collegamento nel menu principale)*: il menu dell'applicazione AVG (*nella parte superiore dell'interfaccia utente principale*) include il collegamento ***Assistenza*** che apre una nuova finestra di dialogo contenente tutti i tipi di informazioni necessarie per ricevere assistenza. La finestra di dialogo include dati di base sul programma AVG installato (*versione programma/database*), dettagli della licenza e un elenco di collegamenti rapidi per l'assistenza.

- ***Risoluzione dei problemi nella Guida***: una nuova sezione ***Risoluzione dei problemi*** è disponibile direttamente nel file della Guida incluso in **AVG AntiVirus** *(per aprire il file della Guida, premere il tasto F1 in qualsiasi finestra di dialogo nell'applicazione)*. Questa sezione fornisce un elenco delle situazioni che con maggiore frequenza spingono un utente a ricercare assistenza professionale per un problema tecnico. Selezionare la situazione che descrive meglio il problema corrente e fare clic sul collegamento per aprire le istruzioni dettagliate per la risoluzione del problema.

- ***Centro di assistenza del sito Web di AVG***: in alternativa, è possibile ricercare la soluzione al problema nel sito Web di AVG (*http://www.avg.com/*). Nella sezione ***Assistenza*** sono contenuti una panoramica di gruppi tematici che trattano problemi commerciali e tecnici, una sezione strutturata di domande frequenti e tutti i contatti disponibili.

- ***AVG ThreatLabs***: un sito Web specifico correlato ad AVG (*http://www.avg.com/about-viruses*) dedicato ai virus, che fornisce una panoramica strutturata delle informazioni relative alle minacce online. Sono inoltre disponibili istruzioni sulla rimozione di virus e spyware e consigli relativi alla protezione.

- ***Forum di discussione***: è inoltre possibile utilizzare il forum di discussione degli utenti AVG disponibile all'indirizzo http://community.avg.com/.